NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UTILIZING CURRENT COMMERCIAL-OFF-THE-SHELF FACIAL RECOGNITION AND PUBLIC LIVE VIDEO STREAMING TO ENHANCE NATIONAL SECURITY

by

Victor F. Cruz

September 2014

Thesis Co-Advisors: Gary Langford
John Osmundson

Second Reader: Daniel P. Burns

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. **AGENCY USE ONLY** *(Leave blank)*	2. **REPORT DATE** September 2014	3. **REPORT TYPE AND DATES COVERED** Master's Thesis	
4. **TITLE AND SUBTITLE** UTILIZING CURRENT COMMERCIAL-OFF-THE-SHELF FACIAL-RECOGNITION AND PUBLIC LIVE VIDEO STREAMING TO ENHANCE NATIONAL SECURITY			5. **FUNDING NUMBERS**
6. AUTHOR (S) Victor F. Cruz			
7**. PERFORMING ORGANIZATION NAME (S) AND ADDRESS (ES)** Naval Postgraduate School Monterey, CA93943–5000			8. **PERFORMING ORGANIZATION REPORT NUMBER**
9**. SPONSORING /MONITORING AGENCY NAME (S) AND ADDRESS (ES)** N/A			10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number _____N/A_____.			
12a. **DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release: distribution is unlimited			12b. **DISTRIBUTION CODE** A

13**. ABSTRACT** (maximum 200 words)

The nation's security depends in part on proactive approaches and methods to evolving technologies for identifying persons of interest, enemies of state (foreign and domestic), potential acts of terrorism, and foreign intelligence. Currently, state and federal entities operate passive surveillance technologies with biometrics to identify and curtail national security threats, so as to act within the confines of the Act for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. However, such surveillance technologies are implemented independently by state and federal agencies, which cause a significant delay in the identification of persons of interest. Consequently, acts of terrorism on U.S. soil as well as U.S. assets abroad that could have otherwise been prevented may occur.

This thesis proposes a generic interoperability technology approach that considers the networking of public live video streaming with state and federal surveillance technologies (including traffic cameras integrated with facial recognition technologies) interlinked with the National Criminal Information Center and Federal Terrorist Screening Database. Requirements surrounding data format and transmission protocols were studied, and concerns regarding existing "need to know" requirements are addressed. The interoperability, or systems of systems approach, and concept of operation is applied to further the enhancement of and fill a capability gap by providing actionable intelligence in real-time using biometrics technologies.

14. **SUBJECT TERMS** Facial recognition, systems engineering, live video streaming, security cameras, national security, terrorist databases			15. **NUMBER OF PAGES** 79
			16. PRICE CODE
17**. SECURITY CLASSIFICATION OF REPORT** Unclassified	18. **SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	19**. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	20. **LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

UTILIZING CURRENT COMMERCIAL OFF THE SHELF FACIAL RECOGNITION AND PUBLIC LIVE VIDEO STREAMING TO ENHANCE NATIONAL SECURITY

Victor F. Cruz
Lieutenant, United States Navy Reserves
B.S., University of Phoenix, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2014

Author: Victor F. Cruz

Approved by: Gary Langford
Thesis Co-Advisor

John Osmundson
Thesis Co-Advisor

Daniel P. Burns
Second Reader

Clifford Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The nation's security depends in part on proactive approaches and methods to evolving technologies for identifying persons of interest, enemies of state (foreign and domestic), potential acts of terrorism, and foreign intelligence. Currently, state and federal entities operate passive surveillance technologies with biometrics to identify and curtail national security threats, so as to act within the confines of the Act for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. However, such surveillance technologies are implemented independently by state and federal agencies, which cause a significant delay in the identification of persons of interest. Consequently, acts of terrorism on U.S. soil as well as U.S. assets abroad that could have otherwise been prevented may occur.

This thesis proposes a generic interoperability technology approach that considers the networking of public live video streaming with state and federal surveillance technologies (including traffic cameras integrated with facial recognition technologies) interlinked with the National Criminal Information Center and Federal Terrorist Screening Database. Requirements surrounding data format and transmission protocols were studied, and concerns regarding existing "need to know" requirements are addressed. The interoperability, or systems of systems approach, and concept of operation is applied to further the enhancement of and fill a capability gap by providing actionable intelligence in real-time using biometrics technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFIS	Automated Finger Print Identification System
AIFIS	Automated Fingerprint Identification System
CIA	Central Intelligence Agency
CJIS	Criminal Justice Information Services
CONUS	Continental United States
CONOPS	concept of operation
COTS	commercial-off-the-shelf-system
DIA	Defense Intelligence Agency
DHS	Department of Homeland Security
DOJ	Department of Justice
ID	identification
FBI	Federal Bureau of Investigations
FISA	Foreign Intelligence Surveillance Act
INLETS	International National Law Enforcement Telecommunications System
LE	law enforcement
LEO	law enforcement operation
MOU	memorandum of understanding
N-DEX	National Data Exchange
NCIC	National Criminal Information Center
NGI	Next Generation Identification
NJI	National Justice Institute
NLETS	National Law Enforcement Telecommunications System
NSA	National Security Agency
PATRIOT ACT	United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
TSDB	Federal Terrorist Screening Database
SOS	system of systems

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The use of facial recognition software to automatically identify persons of interest (POI) (i.e., an individual wanted by state and federal agencies or a person posing a threat to national security) is becoming more commonplace throughout the U.S. As the technology of sensors improves in resolution, miniaturization, and color definition as software becomes more embedded, smaller in code, more extensible and scalable, and as algorithms mature to become more robust and more real-time, the advent of networked sensors providing near-real-time facial recognition for decision makers is nearer. However, there is a technology gap within the community of law enforcement (LE) and decision-makers who want to utilize this technology to share information across domains at the federal, state, and local levels of government to identify a person of interest or to gain evidence in crime investigation (Baker, 2012). This gap between technology and its use is due in part to the accuracy of the current facial recognition capability, the different contexts in which the data is used, and the level of trust that is assigned to the data or to the user. The adoption of facial recognition technology is hampered in comparison to advanced fingerprint technology; facial recognition is not as accurate as the advanced finger print capturing technology (Baker, 2012).

The LE facial recognition process currently in use by some law enforcement agencies consists of first taking a picture of a suspect and then matching the photograph of that person against a photograph of a registered POI stored in a state or federal database. If a match occurs, further action is taken. If no match occurs, the photograph of the suspect is discarded or a new record is generated as a POI. This process is dependent on the circumstances that caused the suspect to be photographed in the first place. In addition, this process currently presents multiple challenges. First, there are time delays in the current process between initiating a search and confirming a match. Second, there is a disconnection between federal databases and state databases because there is not a centralized database where state and federal databases time synchronized information in

widespread use. Finally, most of the information provided by these databases is accessed after a crime has occurred, as that is when the match process is currently initiated by law enforcement.

There are efforts to reduce the time delay it takes for law enforcement to access federal and state databases, but these efforts among all 50 states and all federal agencies are not uniform. Currently, state intelligence fusion cells share information and "mug" shots of active "wanted" and "felons" via the National Data Exchange (N-DEX). The details of N-DEX are discussed in Chapter II. In addition, federal intelligence centers share biometric data, but a query must be made by authorized LE officials to initiate this data sharing. Federal agencies have security requirements in place that do not allow access to all state LE authorities, which complicates matters further.

While state and federal agencies are making an attempt to improve the data-sharing processes amongst themselves by building the N-DEX, currently there is no widespread sharing of biometric data among these agencies because the network infrastructure to support it does not exist. One tragic example and impact of lack of information sharing between state and federal agencies was the shooting incident at Ft. Hood, Texas on November 5, 2009. The shooter was able to purchase a firearm (which requires a state background check) even though he was listed and identified on a federal watch list. At the time, the shooter was being investigated by federal authorities due to his email correspondence with a known terrorist. However, this information was not accessible or available by queries to state law enforcement. Had both state and federal agencies used a common database or shared information, this tragedy may have been averted by preventing the firearm sale. In August 2010, and in response to this event, former Defense Secretary Robert Gates enacted a policy to enable the National Criminal Information Center (NCIC) and the federal Terrorist Screening Database (TSDB) to share information on suspected terrorist threats with civilian agencies and state and local law enforcement (Kenyon, 2010). While the policy set forth by Secretary Gates is undoubtedly a step in the right direction, the current sharing of data is limited and remains passive between state and federal data systems.

This thesis proposes guidelines to improve today's capabilities to interlink live video streaming from various sources and compare with biometrics database servers, which hold details on state and federal criminals. The integrative approach recommended in this research is a system of systems engineering approach to address problems with sharing stored biometric data in near-real time between state and federal authorities. Using commercial-off-the-shelf (COTS) facial recognition technologies and with established need-to-know, the network access and security issues can be addressed. By utilizing active, real-time systems to identify a POI in sensitive areas, law enforcement may be able to prevent criminal activities from occurring or shorten the investigative process by providing relative and timely information to the investigators.

This work begins with a background discussion of the use of biometrics and the current capabilities at state and federal levels. This discussion points out capability gap based on the need for there to be near-real time access to personally identifying information, such as facial imagery and biometrics. The aim of the future information sharing between law enforcement and the intelligence community (LE/IC) is geared toward increasing national security by providing timely and relevant information that will help identify persons of interest who are or maybe a threat to either jurisdictional or national security. In Chapter II, to facilitate these improvements, the link between LE/IC agencies are decomposed into functional relations and then structured as functional flow block diagrams to facilitate the flow of data and information between functions (i.e., relations and potential synergies). COTS technologies for biometrics, still imagery, and live video streaming are discussed in Chapter II.

Also in Chapter II, a concept of operation (CONOPS) for a proposed solution that integrates a network of camera and video systems with a facial recognition system is presented. The discussion explores a system where facial recognition software installed on a remote server, which monitors live video feeds via the Internet, would be used to identify a person of interest that crosses into view of an active public video camera. This would create a master database that would be used by the facial recognition system; this master database would be an integration of the FBI's Criminal Justice Information

Services (CJIS) databases. Such a proposed system will help track, identify, and catalog lifestyle patterns of POIs by recording areas in which the POI has been identified in real-time.

Further research is needed to identify the most advanced technologies available to implement the proposed CONOPS. The focus of this thesis is to identify capability gaps (in terms of interoperability) and to provide a system of systems solution to enhance national security by sharing biometric facial recognition data in real-time utilizing infrastructures currently in place.

It should be noted that the widespread networking of biometric technology for LE/IC with public video systems may meet with issues in regard to social acceptance of the use of such measures, which would result in a lack of support or blocking the efforts to stand up such technology nationwide. While outside the scope of this work, a review of the Executive Order 12333, the Foreign Intelligence Surveillance Act (FISA) and the Act for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) was conducted by the author to ensure that the approach proposed in this thesis fell within the laws defined in these acts. A review of these documents led the author to conclude that the solution presented here would enhance national security while maintaining constitutional rights. While a thorough discussion of the legal issues surrounding the topics discussed in this thesis was out of scope for the present research, the laws relevant to this concept of operation have been reviewed here in order to develop a more complete context.

LIST OF REFERENCES

Baker, T. J. (2012, May). *Biometrics for intelligence-led policing: The coming trends*. Retrieved from http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2358&issue_id=42011

Kenyon, H. (2010, August 24). Gates orders increased data sharing to protect military families.*Government Computer News*. Retrieved from http://gcn.com/articles/2010/08/24/dod-to-increase-data-sharing-to-protect-personnel-and-facilities.aspx

ACKNOWLEDGMENTS

The author would like to thank the brave members of the U.S. military, state and federal law enforcement agencies and the intelligence community who may have sacrificed their lives, time away from home, and luxuries that we take for granted to keep our nation safe. Keep fighting the good fight. I would also like to thank my thesis advisors and all who have supported my journey.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Prior to the events of September 11, 2011 (9/11),law enforcement (LE) and Intelligence community (IC)authorities responsible for protecting citizens from threats against national security were guided by Executive Order 12333 enacted on December 4, 1981, by President Ronald Reagan, the Foreign Intelligence Surveillance Act of 1978, and the National Security Act of 1947. Sharing information prior to 2011 was manpower intensive and caused delays for the LE and IC communities to receive relevant and timely information. There was no electronic infrastructure to support the automatic and seamless sharing of biometric data between state and federal agencies.

After the events of 9/11, there was an immediate need to enhance and amend the aforementioned guiding laws, as they were based on outdated technologies. In order to quickly deter future threats, the Act for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.A. PATRIOT) of 2001 was signed into law by President George W. Bush. The PATRIOT Act has since been extended in 2011 by President Barack H. Obama. In part, the purpose of the act is "to amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes" (Protect America Act 2007).

In addition to 9/11, other national security events have played a role in changing responses to acts of terror and other threats. Specifically, a key episode was a shooting that occurred at Ft. Hood, Texas in 2009. In reaction to this tragic incident, Defense Secretary Robert Gates ordered the creation of a coordinated cyberspace counterintelligence policy to better identify military personnel who may pose a security threat. The shooter, who was listed on a federal watch list for previous suspicious behavior, was able to purchase a firearm without triggering any security alerts. This incident was a stark example of the consequences that may occur given a lack of coordination between state and federal intelligence information. Particularly, the Gates

policy memo notes, "that the services have launched projects to screen personnel who appear on law enforcement databases on NCIC and the TTSD" (Kenyon, 2010). Gates also endorsed using the Law Enforcement National Data Exchange (N-DEx) and the adoption of the Federal Bureau of Investigation's (FBI) eGuardian terrorist threat reporting system to share information on suspected terrorist threats with civilian agencies and state and local law enforcement (Kenyon, 2010).

Concurrently, the FBI has been overhauling its Automated Fingerprint Identity System (AFIS), which currently relies on its agents to input a name of an individual by which to search for a possible mug shot match within the 10-million image database. This outdated system will be replaced with a nationwide facial recognition system as part of a billion dollar Next Generation Identification (NGI) capabilities upgrade. The new facial recognition system was piloted in the winter of 2012 in Michigan, Washington, Florida, and North Carolina. The FBI will implement the full system nationwide in 2014. While clearly an improvement over the current system, this new system retains two legacy attributes that inhibit widespread use and efficiency. The first, the design is for a passive system, and second, "still" photographs, not live video streaming is planned.

B. PROBLEM STATEMENT

The current state of biometrics facial recognition network capabilities varies at the state level. Some states, such as Florida, use facial recognition software, developed by L-1, to share images of suspects among sheriff offices and local police departments to identify and prosecute hundreds of suspects. Other state law enforcement agencies are using software applications installed on smart phones and tablets to quickly take a picture of a suspect and perform an immediate, real-time search to see if there is a match to a known person of interest (POI) (Steele & Angwin, 2011). The use of biometrics by U.S. military personnel abroad to identify persons of interest is similar. Figure 1 depicts an example of biometrics being collected by deployed U.S. military personnel (Schultz, 2012).

Figure 1. Collecting Biometrics by U.S. Military (from Schultz, 2012)

This work proposes a solution for the interoperability gap in the application of facial recognition technologies to public live video feeds to identify persons of interest who pose a threat to national security. The proposed solution also enables information to be relayed to relevant LE/IC authorities in a timely manner. This work also presents a CONOPS that uses commercial-off-the-shelf (COTS) live video feeds along with one of several facial recognition technologies working in concert and interlinking with federal databases to compare and identify matches of persons of interest for further action. It is hoped that this CONOPS (if researched further and tested) could be used to identify a POI before a criminal event occurs or alert relevant LE officials that a POI is in their area. This solution introduces a proactive use of facial recognition biometrics rather than the reactive approach that has been implemented to date. An additional benefit of the CONOPS presented here is to guide LE / IC components to invest in developing the "interlink gap" since time and money has already been spent by the public on the available Internet infrastructure.

C. THESIS OUTLINE

An overview for each chapter is presented below. Each chapter supports the previous chapter through applying the systems engineering process.

1. Chapter I: Introduction. Chapter I introduces the high-level problem this thesis addresses and identifies the problem statement that is used as the foundation of this document.

2. Chapter II: Current Law Enforcement Capabilities. Chapter II presents an overview of the federal organizational structure of the IC. The FBI was chosen as the primary subject in this discussion: in the FBI's Criminal Justice Information Services Division is advanced in its use of biometric database management. Chapter II discusses the national fusion centers at the state level, particularly how the various states each take a diversified approach in biometric facial recognition crime fighting.

3. Chapter III: System of Systems Interoperability Approach. Chapter III presents the systems of systems (SoS) approach and discusses why the interoperability model was chosen as the process for architecting and presenting the networked, national security facial recognition system.

4. Chapter IV: National Security Network Hypothesis. Chapter IV proposes a solution to the identified capability gap. The detailed decomposition of an interoperability model is presented. A step-by-step description is presented that identifies a groundbreaking approach to improving the ability to identify persons of interest who are threats to national security. This approach also identifies a means to quickly disseminate vital information that enables law enforcement authorities to be proactive rather than reactive in combating national security threats.

5. Chapter V: Conclusions and Summary. Chapter V summarizes the recommendation for the need for further research to develop a networked facial recognition system for the identification of persons of interest in close to real time, and touches upon the possible future research for the expansion of the system including other identification technologies. In addition, this chapter reviews the need and concept for the proposed system and the benefits associated with this system.

II. CURRENT LAW ENFORCEMENT CAPABILITIES

This chapter describes current federal and state systems in place for the identification of persons of interest via facial recognition technologies. Of particular interest in determining the improvements necessary for the implementation of a network to share data and information within the community of law enforcement and decision makers is the identification of the requirements for each localized non-networked system. In addition, the technology gap is typified by exposing the existing limitations of each system and developing the roadmap (s) to provide appropriate levels of interoperability for each system. In addition, the current state-of-the-art in COTS facial recognition systems and live video streaming are described.

A. FEDERAL LAW ENFORCEMENT USE OF BIOMETRICS

In this section, the current federal LE/IC capabilities in the area of facial recognition and how it is used in the defense of national security are described. The FBI's state-of-the-art facilities with regards to biometrics are presented, as the FBI leads the way in developing the most sophisticated facial recognition program, parts of which are being deployed nationally. The facial recognition system is part of the FBI's $1 billion Next Generation Identification (NGI) program, which is an initiative built around the use of biometric data such as facial recognition and more sophisticated finger print analysis. In addition, this initiative includes the use of other types of biometric data to identify suspects, such as palm prints and tattoos, and potentially even DNA. According to the FBI, the biometric technology will be used for:

1. Identifying fugitives, missing persons, and unknown persons of interest,
2. Tracking movements to/from critical events,
3. Conducting automated surveillance at lookout locations (e.g., Occupy Wall Street events), and
4. Verifying mug shots against National Criminal Information Center (NCIC) records. (Reardon, 2012)

The full NGI program, slated for full completion by 2014, is expected to provide faster, more efficient law enforcement. In addition to more efficiently identifying criminals after a crime has occurred, the system puts in place technologies that could enable enhanced capabilities that could stop offenses before they occur (Reardon, 2012). Early tests on limited amounts of data (1.6 million mug shots) have shown the facial recognition system component correctly identifies individuals with 92 percent confidence rating, and the system is capable of operating on a database with up to 12.8 million mug shots (Endler, 2012).

Since the FBI is not alone in its charge to protect national security, other agencies are important to consider in this analysis. There are currently 17 agencies within the IC that have some form of national security protection responsibilities. The Director of National Intelligence (DNI) serves as the head of the IC. Figure 2 shows the members of the IC and its leadership, and the Appendix provides an overview of their responsibilities.

Figure 2. Organization of the Director of National Intelligence (from *Wikipedia*, 2013)

1. Introduction

The capabilities of the FBI are detailed in this chapter, as this agency has the greatest and most advanced biometric capabilities in the continental U.S. (CONUS). The Criminal Justice Information Service (CJIS) is the largest department within the FBI and home of the nation's largest biometric repository. It houses the fingerprints and criminal histories for more than 70 million subjects in criminal master files, as well as 34 million civil prints (FBI, 2012b). For reference, **Error! Reference source not found.** illustrates an historical timeline of the relevant laws that have governed the use of biometrics from the inception of the FBI in 1905 to the present. The Security Act of 1947, the Foreign Intelligence Surveillance Act (FISA) of 1978, Executive Order (EO) 1333 of 1981, and the PATRIOT Act of 2001 (plus revisions) are the operative policy guidelines that form the basis for the network sharing concept proposed in this thesis.

A key design requirement for the proposed network-sharing concept is that it be on a flexible architecture that can remain responsive to changes in national policy. That flexibility will be ensured by "common access" protocols (CAPs) that determine the necessary credentials needed for accessing various types and sources of data and information. Those CAPs will be centrally control by the FBI (pick an office or designation to lend credibility to this statement) and will comply with the laws and guidelines promulgated by national security policy.

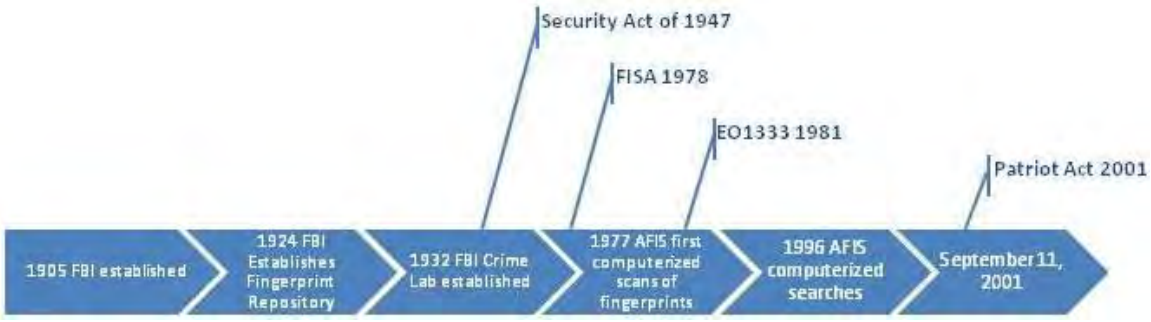

Figure 3. FBI Timeline and Relevant Security Acts

2. Relevant FBI Offices and Capabilities

The National Security Branch (NSB) of the CJIS was established on September 12, 2005, in response to a presidential directive issued by President George W. Bush for a national security service that combines the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI under the leadership of a senior FBI official (FBI, 2012d). The NSB's purpose is to strengthen the integration of the FBI's intelligence and investigative missions. Information collected through FBI investigations is analyzed, not just to build a case for prosecution, but for its predictive value. In turn, intelligence and gap analysis drives investigative strategies. In July 2006, the Weapons of Mass Destruction (WMD) Directorate was created within the NSB to integrate WMD components previously spread throughout the FBI (FBI, 2012d).

In addition to managing and maintaining the databases used for national security, the CJIS has a number of sophisticated identification capabilities. Relevant to this work is the integration of CJIS's Advanced Fingerprint Identification Technology into the Integrated Automated Fingerprint Identification System (IAFIS) as part of the NGI program. Improvements slated for the IAFIS system include faster and more efficient identification processing, increased search accuracy, improved latent processing services, and allowing for seamless searches of 10-flat finger print impressions for noncriminal justice purposes, such as criminal background checks for employment purposes.

In addition, the Repository for Individuals of Special Concern (RISC) is a national mobile identification system that provides law enforcement and partnering agencies with rapid/mobile identification services of FBI most wanted persons, suspected terrorists, and sex offenders. The RISC system is optimized to provide very quick access to information based on the level of threat that an encountered individual may pose. Figure 4 illustrates the FBI's fingerprint ID process in detail (FBI, 2012a).

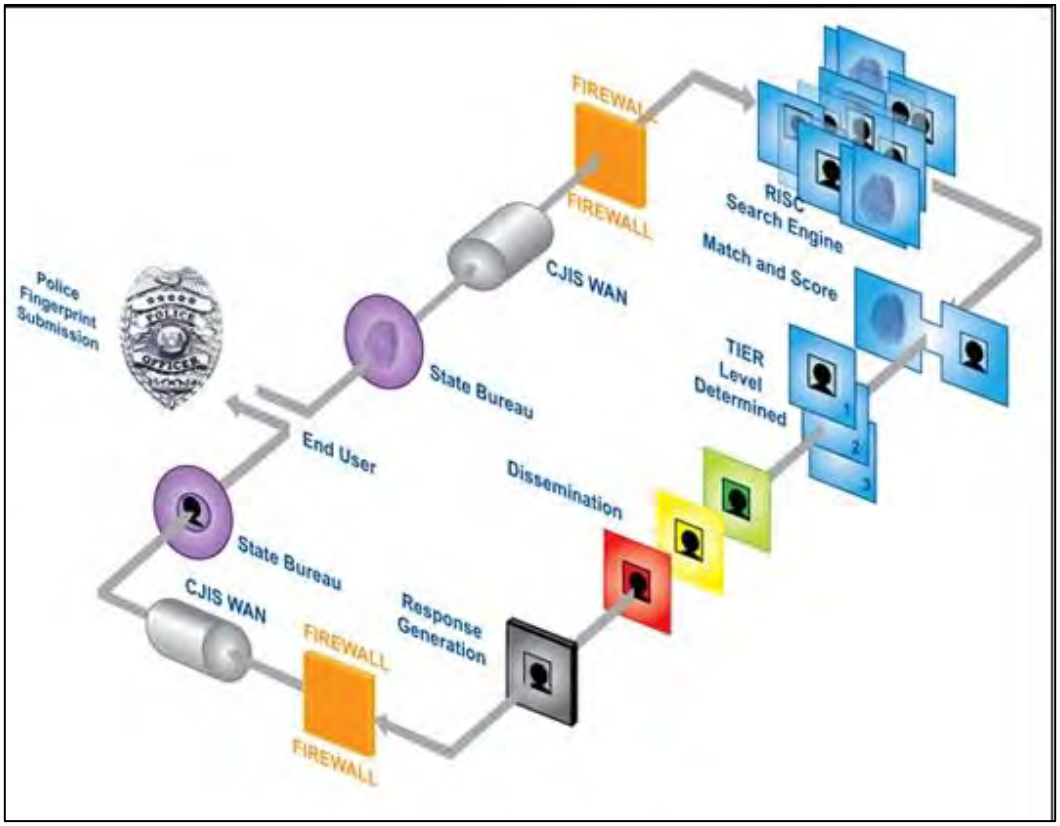

Figure 4. FBI RISC Process Flow Diagram(from Mayo, 2011)

The RISC system allows LE to access and share information via the World Wide Web in addition to the existing data terminals. Improvements to the RISC system have reduced response times by 92 percent for urgent need criminal investigations (reducing a two-hour response time to 10 minutes) and 99 percent for urgent civil requests (reducing a 24-hour response time to 15 minutes) (FBI, 2012a). The RISC system contains a subset of the national fingerprint repository, which is comprised of biographical and fingerprint information that is associated with wanted persons, known or suspected terrorists, sex offenders, and other identified POI. Currently, the RISC system stores approximately two million records (FBI, 2012a). LE can identify a person of interest quickly by the use of a mobile fingerprint device connected wirelessly to the NSIC system (Mayo, 2011). In

addition, local LE can scan a fingerprint from a suspect and within a minute receive detailed information about the subject if there is a fingerprint match against a registered POI.

The CJIS is also home for the National Crime Information Center (NCIC), which provides over 92,000 LE authorities and users with information on over 11.7 million active records (FBI, 2012c). The information available for access includes missing, wanted, and unidentified persons, as well as particulars on stolen property. Moreover, new capabilities added to NCIC in 2011 include a license plate reader (LPR) to assist in recording license plates and access to "screen" plates of moving and parked vehicles to deter and apprehend vehicle theft offenders. **Error! Reference source not found.** lists the information that is currently available to LE/IC under NCIC (FBI, 2012c).

Personal Records	Property Records
Convicted Sex Offenders	Firearms records / loss –missing
Criminal conviction records	Stolen, embezzled counterfeit securities
Foreign fugitives	Stolen property
Immigration violators	Stolen vehicles / boats
Missing persons	
Parolees or people on supervised release	
Active arrest warrants	
Domestic violence protection orders	
Secret service protective alerts	
Terrorist organizations & memberships	
Unidentified human remains	
Violent gang and organizations	

Table 1. National Crime Information Center Record Types (after FBI, 2012c)

While specific records are not available for public viewing, examples of data included in these records types are:

- Vehicle file: records on stolen vehicles, vehicles involved in the commission of crimes, or vehicles that may be seized based on federally issued court order.
- Foreign fugitive file: records on persons wanted by another country for a crime that would be a felony if it were committed in the United States.

- Known or suspected terrorist file: records on known or appropriately suspected terrorists in accordance with *Homeland Security Presidential Directive 6* (HSPD-6).

Other databases and services that provide law enforcement with near real-time data upon request are the National Instant Criminal Background Check System (NICS), Law Enforcement National Data Exchange (N-DEx), CJIS Division Intelligence Group (CDIG), Law Enforcement Online (LEO), and the Uniform Crime Reporting (UCR) Program. Figure 5 illustrates the complete CJIS infrastructure.

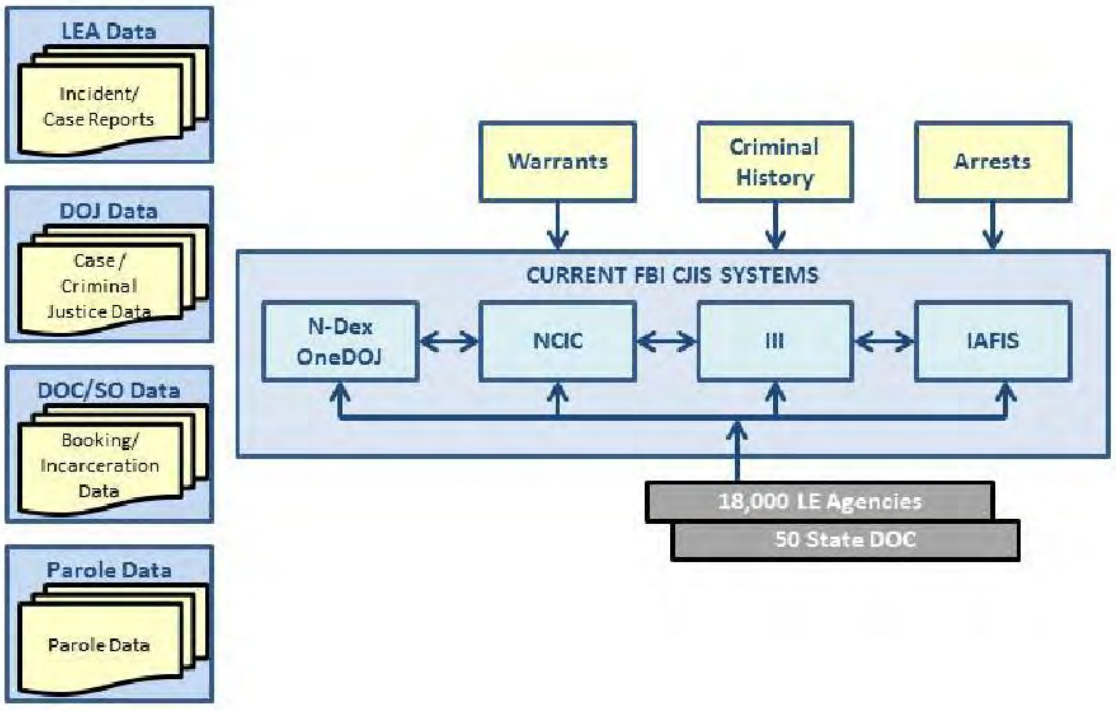

Figure 5. Criminal Justice Information Services Division Capabilities (from FBI Criminal Justice Information Services Division, 2009)

The FBI CJIS systems provide data to 18,000 LE agencies and all 50 state Department of Corrections agencies. The development of the N-DEx has allowed for seamless access to previously segmented data systems, namely the National Crime Information Center (NCIC), Interstate Identification Index (III) and the Integrated

Automated Fingerprint Identification System (IAFIS). The NDEx brings together the data sources listed on the left of **Error! Reference source not found.**, such as incident and case reports, booking, and incarceration data, and parole/probation data from LE agencies. This integration of such data has never been available before, and it allows for the detection of relationships between people, vehicle, property, location, and crime characteristics. Information stored in the N-DEx is searched via an easy to use web-based application, which allows subscribed users to specify search terms in flexible ways to locate potential matches. It has full text search capabilities (e.g., bike gang Riverdale Maryland), as well as the ability to conduct more complicated search queries that take into account geospatial information (e.g., nearest to, within a region) and exclusion terms (e.g., tattoos NOT Delaware) are supported.

In special relevance to this work, the system also provides subscription service capabilities so that a user can set up a subscription and be notified automatically if certain criteria are satisfied. For example, a subscription can be set up to notify a user if a record is submitted to N-DEx that matches a specific person. This provides a proof point that the automatic notification of match events to disseminate to interested users. This is a capability that is a key requirement for the CONOPS proposed in this thesis.

In March 2004, the FBI created its consolidated terrorist watchlist by merging separate watchlists previously created and maintained by a variety of agencies within the federal government (FBI, 2009). The watchlist is used by screening personnel at U.S. points of entry and by federal, state, and local LE officials. This list serves as a critical tool for these personnel by notifying the user of possible encounters with known or suspected terrorists and by providing instruction on how to respond to the encounter. The watchlist is updated with new information gathered by U.S. intelligence and LE agencies (FBI, 2009).

3. Watchlist Nomination Process

As fully described in the U.S. Department of Justice audit report 09-25, May 2009, the relevant details of the FBI's terrorist watchlist nomination process is presented below.

According to FBI policy, all subjects of FBI international terrorism investigations must be nominated to the consolidated terrorist watchlist, including persons who are under preliminarily investigation to determine whether they have a nexus to terrorism. FBI policy also states that all known or suspected domestic terrorists who are subjects of FBI full investigations must be nominated to the watch list. Under certain circumstances, FBI policy also allows for the nomination to the watchlist of known or suspected terrorists for whom the FBI does not have an open international terrorism investigation. For example, the FBI may obtain information about a known or suspected terrorist residing outside of the United States for whom it believes watchlisting is warranted, but for whom it has no open terrorism investigation because there is no known nexus to the United States.

> Whenever an FBI field office opens a preliminary or full international terrorism investigation or a full domestic terrorism investigation, the field office must notify certain Department of Justice (DOJ) and FBI headquarters units of the case opening within 10 working days. One of the FBI headquarters' units that must be notified is the FBI's Terrorist Review and Examination Unit (TREX). TREX is the FBI headquarters unit that serves as the processing unit for almost all FBI watchlist nominations resulting from open FBI terrorism investigations. In order for TREX to process an initial watchlist nomination, the assigned case agent must electronically submit copies of the opening electronic communication document (which formally opens the case within the FBI), the notice of initiation (which formally notifies DOJ of the case opening), and a watchlist nomination form. (FBI, 2009, p. 4)

The same FBI document also explains:

> For both international and domestic terrorist nominations, TREX is responsible for reviewing and approving each nomination. TREX's quality assurance review verifies that there is justification for the nomination, that the information submitted is complete and accurate, and that the criteria are met for inclusion of the subject in downstream databases. (2009, p. 4)

The procedure is explained by the 2009 FBI document as:

> Once TREX has reviewed and approved a watchlist nomination, it sends the nomination of known or suspected international terrorists to the National Counterterrorism Center (NCTC) branch, staffed by FBI personnel, which reviews the nomination and enters it into its Terrorist Identities Datamart Environment (TIDE) database. Each weeknight and twice on Fridays, the NCTC performs an electronic export of the known or suspected terrorist information in TIDE to the FBI's Terrorist Screening Center (TSC). The TSC then performs one final quality review of the new records before importing them into the TSC's consolidated terrorist watchlist, which is also known as the Terrorist Screening Database (TSDB). Like the NCTC, the TSC conducts a nightly electronic export of the TSDB that sends the watchlist information to the various screening databases used by the U.S. government and some of its allies. (pp. 4–5)

The nomination process for known or suspected domestic terrorists differs slightly in that TREX submits these nominations directly to the TSC. The NCTC is not involved in the process because its TIDE database is prohibited from containing purely domestic terrorism information (FBI, 2009, p. 4).

Figure 6 illustrates the described enrollment process for a person of interest to be included in the terrorist watch list. Typically, it takes up to 20 calendar days (taking into account weekends and holidays) to post information on the terrorist watchlist and populate that information across all federal LE databases. As indicated in Figure 6, this time includes up to 10 working days for the field office work, 24 hours for TREX, 24 hours for NCTC, and 24 hours for the TSC (FBI, 2009, p. 13).

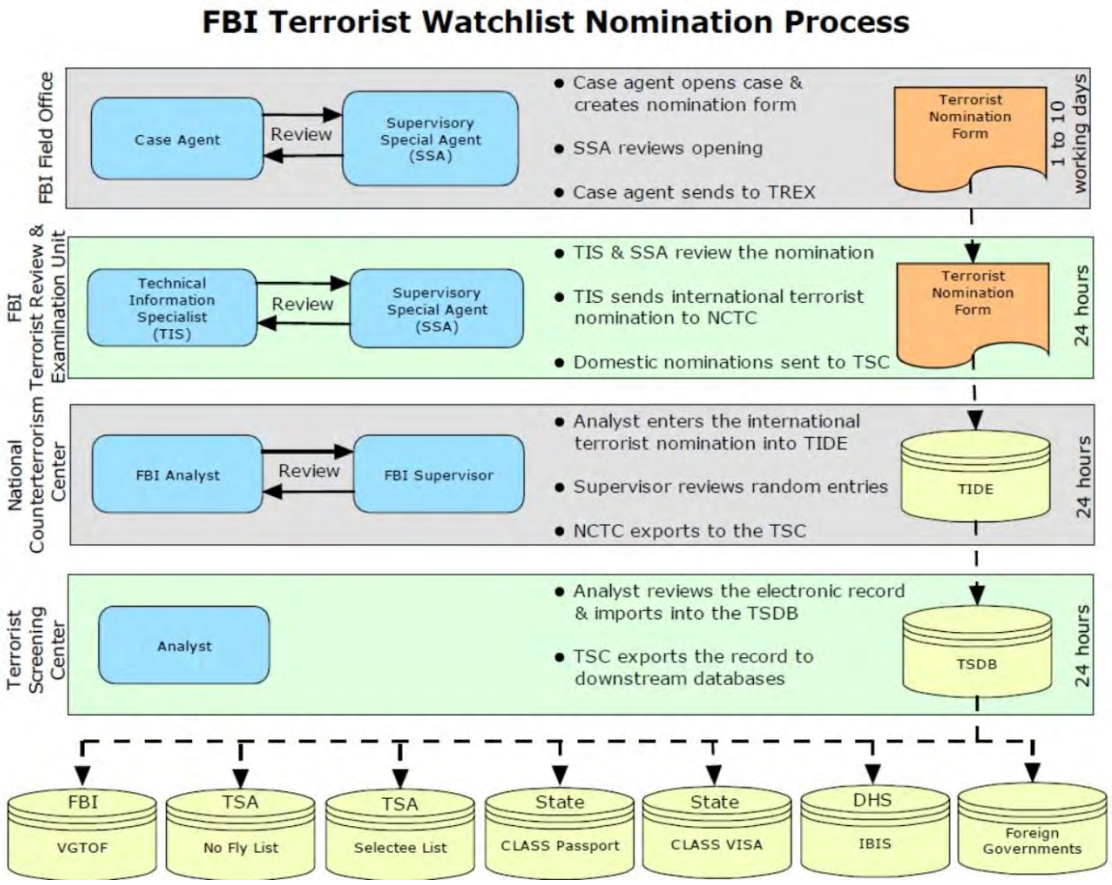

Figure 6. Terrorist Watch List Nomination Process (from FBI, 2009, p. 13)

As of September 2008, over 400,000 unique names and over 1,000,000 records are contained in the database (FBI, 2009, p. 86). Once a person has been entered into the FBI terrorist watchlist system (and therefore tagged as a POI), the POI is typically identified in one of three ways:

1. upon physical sighting of the POI,
2. through active surveillance, or
3. via intelligence information collected from the LE or IC. Each of these activities require some form of human involvement (i.e., personnel actively watching areas for which security is a concern).

Even when using camera feeds, which allow a single individual to watch multiple areas via the monitoring of those feeds, the process is prone to error and the task is difficult to maintain for any length of time. In addition, members of the LE/IC

community cannot be everywhere at once, which means that some POIs will go unnoticed. The introduction of technology that can automatically scan for and identify POIs and return match information to appropriate members of the LE/IC community could increase detection rates and act as a force multiplier to traditional surveillance techniques. That is, automated systems would effectively increase the number of "eyes" on a monitored security area or expand the number of areas that could be covered.

A logical extension to the existing CJIS infrastructure and capabilities is to enable an automatic, real-time system to identify POIs based on input from existing security video camera feeds. This thesis proposes adapting the infrastructure that is mostly in place today to assist LE/IC in identifying POI, including the POI's location.

B. STATE LAW ENFORCEMENT COMPOSITION

In this section, the current state LE/IC capabilities in the area of facial recognition is described and how that information is used in the defense of national security through collaboration between state and federal agencies.

In 2003, DHS teamed up with the DOJ to initiate the National Network of Fusion Centers across the country (DHS, 2012). The main purpose of these fusion centers was to disseminate terrorism threat information from federal law enforcement authorities to state and local authorities and law enforcement agencies. DHS set up a system called Suspicious Activity Reporting (SAR) Initiative (SNI) to allow state and local law authorities to report and respond to counterterrorism activities. The main goal of the SNI is to assist participating agencies in adopting compatible processes, policies, and standards that foster broader sharing of SARs, while ensuring that privacy and civil liberties are protected in accordance with local, state, and federal laws and regulations (Fusion Process Catalog of Services 2011).

According to the U.S. Department of Homeland Security (2012) "National Network of Fusion Centers Fact Sheet," state and major urban area fusion center serve as primary locations within the state and local areas for the receipt, analysis, gathering and sharing of threat-related information among federal, state, and local partners. Fusion

centers conduct analyses and facilitate information sharing, and they are owned and operated by state and local entities with support from federal partners. These centers are uniquely situated to empower frontline personnel to understand the local implications of national intelligence by providing tailored, local context to national threat information. To date, the 72 existing fusion centers range from less that range in age from than one year to 10 years old, with most between four and six years old. They range in size from three staff members over 100 staff members in large centers, with an average fusion center size of 25 staff members (U.S. Department of Homeland Security, 2011).

State and local LE/IC authorities are taking proactive steps in sharing biometric data. Several states have a dedicated network in pilot stages where all LE/IC officials from state police, local city and town police, and county sheriff officers have the ability to collaborate and quickly query information from their patrol cars. For example, products like eAGENT provide access to criminal justice data from local, federal (including the FBI N-DEx data) and interstate data from the mobile data terminals installed in patrol units. Moreover, New Mexico, Arkansas, Florida are among the states using the eAGENT system (eAGENT Client Mobile, 2012).

In addition, COPSync is providing similar capabilities to hundreds of municipal and county law enforcement agencies in more than 150 of the 254 Texas counties (COPSync, 2012). Through a collaborative effort with the state of Michigan, Oakland County's Courts and Law Enforcement Management Information System (CLEMIS) participates in Michigan's Local Government Network, the Michigan Incident Crime Reporting database, and Michigan fusion centers to consolidate crime reporting and biometric data. Furthermore, CLEMIS makes this data available to all participating agencies throughout the state. One of the two key components of the data shared by CLEMIS is Mugshots, the CLEMIS biometric imaging system. This system provides the public safety community with immediate access to mug shot images and other data (i.e., images of scars, distinctive marks, tattoos) through desktop computers, patrol vehicles, or wireless devices (Bertolini, 2012).

Other states, such as Florida, are using facial recognition technologies to assist in capturing local and state fugitives. In Florida, Tampa Police set up cameras at the turnstiles at Super Bowl XXXV and took pictures of everyone who entered (Chachere, 2001). These pictures were screened against a database of known criminals and international terrorists. The facial recognition system was loaned to them by Viisage Technology (now L-1 Identity Solutions) based in Littleton, Massachusetts (L-1 Identity Solutions, 2012). Tampa Police Dept. recorded 19 matches for POI with active warrants thus proving the technology works.

Other state LE/IC departments are using handheld facial recognition systems as identified in **Error! Reference source not found.** (Steele & Angwin, 2011). This system allows a police officer to take a picture of a suspect that is then compared against a repository of active criminals on wanted lists. A positive ID can result in a quickly executed apprehension by the police officer. This operational concept outlines a scenario that captures many of the requirements for the front-end stage of the CONOPS proposed in this work. Details of these requirements will be discussed in Chapter IV.

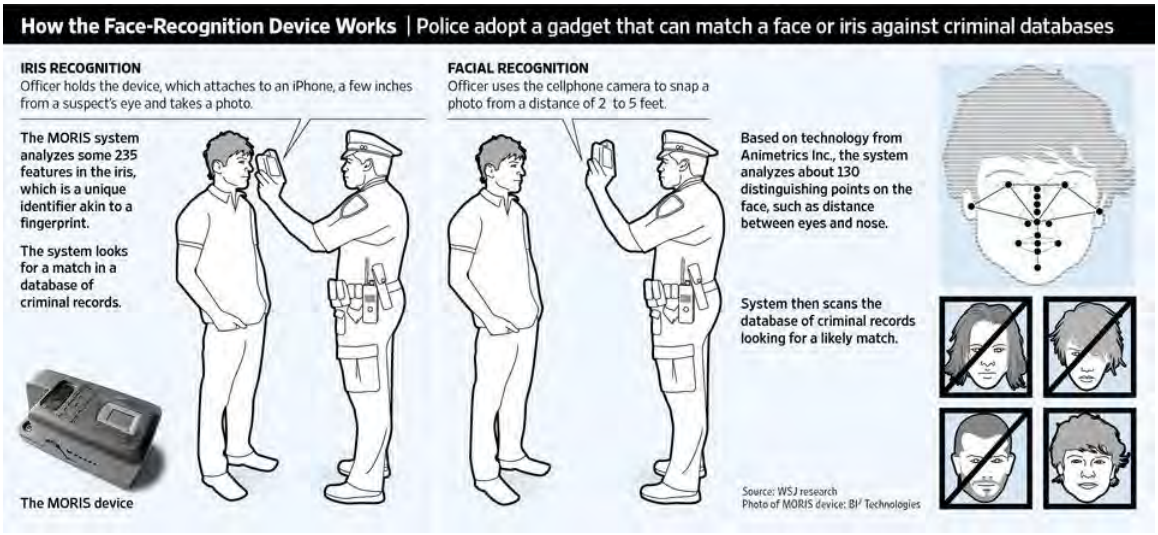

Figure 7. Police Processing Suspect with Handheld
(from Steele & Angwin, 2011)

C. COMMERCIALLY AVAILABLE RELEVANT TECHNOLOGIES

This section will discuss the relevant commercially available technologies and how they may be used in the defense of national security, namely, facial recognition and CCTV systems. Note that section is not an endorsement of any specific company or technology, but rather it is a summary of the types and kinds of technologies that are available today. Until such time as the government has given authority to an acquisition professional to request information from a vendor, information, such as is included in this section, suffices to illustrate a general capability. It is outside the scope of this thesis to review the state of the art of technologies that are found commercially and that could be leveraged and integrated into an active facial recognition system.

1. Facial Recognition

The following is a summary of three providers of facial recognition technology that illustrate a relatively current technology.

a. Progeny Systems Corporation

Progeny's product, Surveillance, Persistent Observation, and Target Recognition (SPOTR), is a biometrics facial recognition system under development that is purported to detect, track, and identify non-cooperative targets utilizing a video sensor network (SPOTR Corporation, 2013).

b. West Virginia High Tech Consortium

West Virginia High Tech Consortium (WVHTC) is developing an advanced biometrics facial recognition system called Tactical Analysis of Video Imaging (TAVI) with funding from the Office of Naval Research (ONR). First demonstrated at Empire Challenge, Ft. Huachuca, Arizona, TAVI is purported to have evolved to enable identification of non-cooperative targets through CCTV systems (Advanced Technology Group: Tactical Analysis of Video Imagery, 2013).

c. Safran / Morpho Trust (Formerly Viisage)

As mentioned above, Viisage provided the biometrics software system used in Super Bowl XXXV ostensibly to help prevent domestic terrorism. The camera systems captured images of ticket holders as people entered the stadium. The images were then compared against those of known criminals and international terrorists (Biometrics, 2013). Although both Progeny System Corporation's SPOTR and the WVHTC TAVI system are currently in research and development (R&D) phases of development, both companies are purported to be moving toward ruggedized, deployable systems.

2. CCTV

a. Internet Public Live Stream Video

Opentopia (Free Live Webcams, 2013) Dropcam, Inc. (Public Dropcams, 2013), and EGGMAN Technologies (Mobile Surveillance, 2013) all are supposed to provide free access to various cameras that have the correct drivers and are connected to the Internet. Provided access includes video feeds from public places as well as personal camera feeds. These CCTV systems are claimed to be starting to provide HD quality imagery, which further increases their usefulness as data feeds for recognition systems.

b. Traffic Cameras Are Provided by State Department of Transportation Websites

Examples of traffic camera feeds available can be viewed at www.trafficland.com or state Department of Transportation (DOT) websites directly. **Error! Reference source not found.** depicts a traffic camera that is viewable from the Virginia State DOT website. While currently the quality of video collected by traffic cameras is low, upgrades to HD quality video are likely to be rolled out in the future and then these feeds will become a more viable option for facial recognition purposes.

Figure 8. Department of Transportation Camera

c. Other Private and Government Furnished Sources

There are many additional video sources that could be used as data feeds for the proposed system. To utilize feeds from security cameras at stores, parking garages, airports, or and other high threat areas, the video feeds would need to be integrated into a secure WAN. **Error! Reference source not found.** is an example of some security camera images.

Figure 9. Examples of Other Security Cameras

D. INTERNATIONAL TRENDS

In addition to its increased use in the U.S., cataloging biometric data for law enforcement purposes is becoming more prevalent internationally. In Australia, the New South Wales (NSW) government began recording features for facial recognition purposes in 2010, using driver's license photos (Jones, 2010). At this time, every person who walks past a CCTV can be tracked throughout the city. Similar to how it is in the United States, in Australia, each state and territory is responsible for maintaining law and order within its borders. CrimTrac is the national information sharing service for Australia's police, law enforcement, and national security agencies. It provides services for information sharing by partnering with Australia's police agencies. These partnerships enable CrimTrac to provide information to police across state and territory borders. Furthermore, CrimTrac has asked NSW for its facial features database so it can be mined nationally by police using the facial recognition technology (Jones, 2010).

E. SUMMARY

State LE and IC authorities are beginning to share criminal information through the advanced capabilities of the FBI's CJIS. In addition, the LE and IC communities are making great strides in the identification and apprehension of suspects with the use of shared biometric data, including facial recognition. The FBI's NGI program has a

specific task of integrating facial recognition into its capabilities. NGI Increment 4, slated for full deployment in the summer of 2014, includes a new facial recognition system. It was initially piloted in February of 2012, providing a search of the national repository of photos consisting of criminal mug shots. Currently, this repository contains approximately 12.8 million searchable frontal photos (Endler, 2012). The pilot program permitted authorized LE agencies to submit queries for a search of the repository of mug shots, and the results of the search were returned to the submitting agency as a lead in the form of a ranked list of candidate matches.

In February of 2012, the state of Michigan successfully completed an end-to-end Facial Recognition Pilot program and is currently submitting facial recognition searches to CJIS (*What Facial Recognition*, 2012). The pilot program is open to states or agencies that already have established facial recognition systems. Hawaii, Maryland, South Carolina, Ohio, and New Mexico either already have a memorandum of understanding (MOU) in place or are engaged in the MOU review process for pilot participation. Kansas, Arizona, Tennessee, Nebraska, and Missouri are also interested in pilot participation before the full program roll-out in the summer of 2014 (*What Facial Recognition*, 2012).

The use of this technology, even in the ground breaking NGI system, requires a LE official as part of the process. The LE official must gather his/her own photo evidence and submit that data via a query to the CJIS system. Typically, this process occurs after a crime has been committed. By creating an automated process, the integration of networked security camera systems into the process of submitting photos or by streaming video automatically to the facial recognition system provides a solution where LE officials are alerted of the presence of a POI *before* a crime is committed.

The technology to support the automation of the detection of POIs by using security camera systems is currently available, both for the facial recognition capabilities and for the video capture capabilities. A successful implementation will likely require an upgrade to the existing video camera equipment as many of the installations in place today are of low quality. However, the feasibility of this approach has already been

successfully demonstrated on a smaller scale internationally. In the following chapters, a proposal that utilizes much of the existing infrastructure is introduced to include such capabilities in CONUS. Figure 10 illustrates how this implementation could augment the CJIS current capabilities with the existing capability gap clearly indicated.

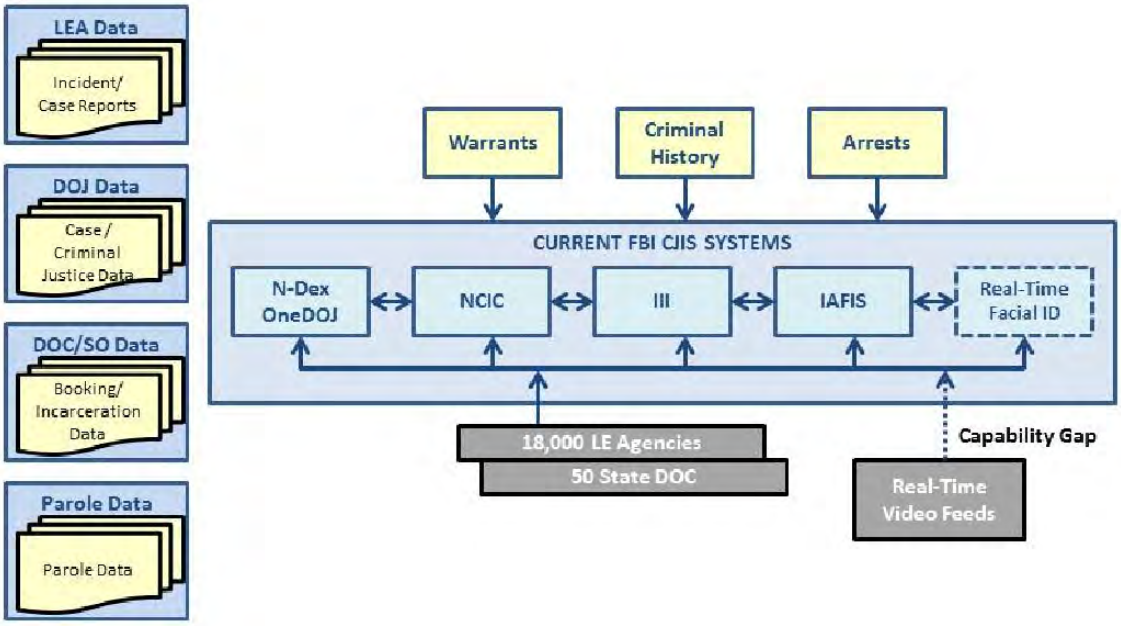

Figure 10. CJIS Capabilities Augmented with Proposed Work

III. SYSTEM OF SYSTEMS INTEROPERABILITY APPROACH

This chapter introduces the system of systems and interoperability approaches adopted in this work. In addition, a discussion of a system of systems' spiral development cycle is suggested for use in the development of the solution. The following chapter shows how these approaches relate to the CONOPS proposed in this thesis. There are multiple definitions of a system of systems (SoS) engineering approach. Kaplan's definition is one that applies well to this thesis (Kaplan, 2006). This approach is summarized as follows:

> A system-of-systems is a large, complex, enduring collection of interdependent systems under development over time by multiple independent authorities to provide multiple, interdependent capabilities to support multiple missions. (Kaplan, 2006, p. 16)

In addition, the term "interdependent" is defined by Kaplan (2006) as "the senses that mission success requires that they work together, and that their features or attributes may be traded off against each other" (p. 16). This particular definition of a system of system and interdependence is helpful to have in mind for this thesis research. This is because in order for the concept of operation that will be presented in this research project to work, all required subsystems (e.g., the network infrastructure, camera and live video feeds, reporting infrastructure, facial recognition system) of the proposed architecture must be interdependent to achieve the goal of identifying a person of interest who might pose a threat to national security in near real time. The sum of the subsystems in this thesis architecture is large and complex, something that also fits into the definition offered by Kaplan.

In addition to being a SoS, the components of the architecture presented in this thesis need to be interoperable. In common terms, interoperability is the process of taking diverse systems and enabling them to work in concert. The article "Identifier Interoperability: A Report on Two Recent ISO Activities," provides a formal definition of interoperability:

> The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together to mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate. (2012)

A. DEVELOPMENT CYCLE

Error! Reference source not found. illustrates the system development cycle process for a complex system such as the one proposed in this work (i.e., one requiring system interoperability). The various components of this process are discussed in detail in this chapter. The following chapter discusses how they apply to the implementation of the CONOPS presented in this thesis.

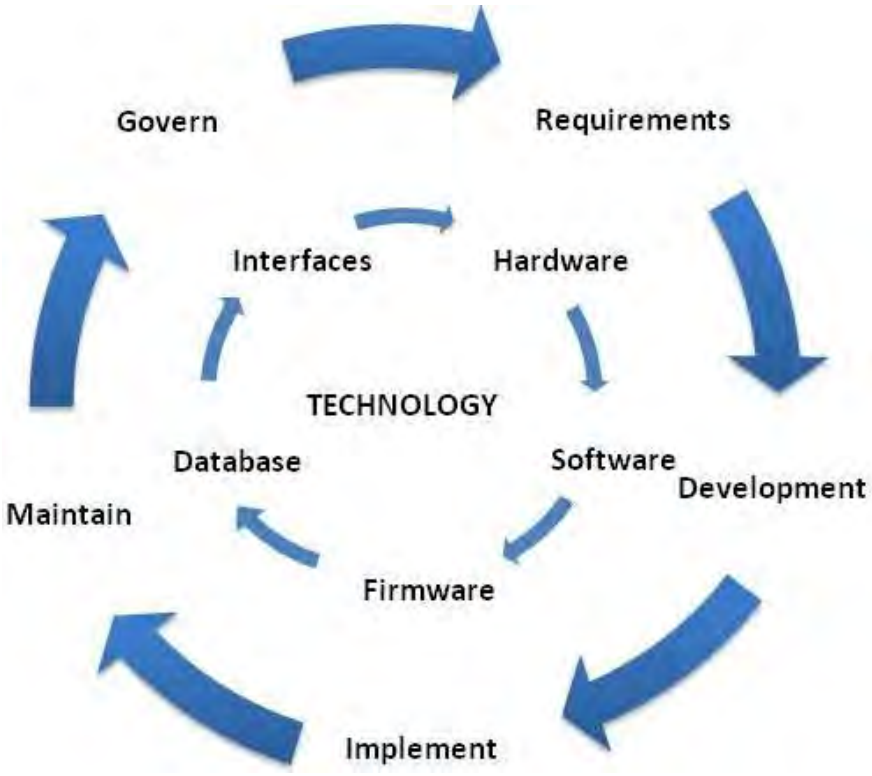

Figure 11. Cyclical Development Model (after Boehm, 1986)

1. **Requirements**. During the requirements phase, system needs are identified and clearly defined. Hardware and software specifications are

initially defined, stakeholders (lead agencies) are identified, and funding requirements and sources are also identified.

2. **Development**. During the development phase, working groups are established, statements of work are clearly defined for each working group, risk analysis is conducted and a preliminary system is developed.

3. **Implement**. During the implementation phase, pilot programs are started, and system and acceptance testing is completed. Feedback from stakeholders is taken into account and the system is modified to ensure the system performance meets the stated requirements.

4. **Maintain**. During the maintenance phase, the primary stakeholder is responsible for the life cycle support throughout the life of the program. Training must be established to allow the users to operate the system for its intended purpose. Lessons learned are also brought forward during this phase to help guide any future related development.

5. **Govern**. During the governance phase, the implemented technology is monitored to ensure system performance meets the defined requirements, governing policy is refined, and life cycle technology updates are defined. (Boehm, 1986, p. 14)

As illustrated by the inner cycle depicted in the development cycle in **Error! Reference source not found.**, the impacted technology components include system hardware, software, firmware, and the underlying databases and interfaces associated with the system implementation. Each of these technological components must be considered during each phase of the cycle. For example, requirements must be detailed for all required system hardware, software, firmware, databases and interfaces during the requirements phase of the cycle. Plans must be put in place to monitor the system performance of the facial recognition system implemented during the governance phase to ensure the system meets the defined requirements.

B. SPIRAL DEVELOPMENT MODEL

The cyclical development model introduced in the previous section defines the process to be followed as a whole to develop a complex system of systems program. To efficiently implement each individual system as well as the integration effort, the spiral method is recommended. The spiral method (implemented by the spiral development model) was developed by Barry Boehm and provides a risk reducing approach to the software development life cycle (Boehm, 1986). The model blends elements of both

design and prototyping in stages to combine the advantages of top-down (waterfall) and bottom-up (prototyping) models commonly used in systems development. The spiral model is intended for large, expensive, and complicated projects, such as that proposed in this work.

The spiral development model is illustrated in Figure 12. Each loop in the spiral represents a development phase. Depending on the complexity of the project, there may be multiple development phase loops as initial prototypes are further developed and evaluated against requirements. Each loop traverses through four quadrants, where the following activities take place:

1. Determine objectives, alternatives, constraints: Regardless of how far we are in the development process (i.e., what loop we are on), we must define the objectives, determine available alternatives, and assess the constraints of the given cycle. This process ensures that we are developing to our overall requirements and will stay focused on the important aspects of the particular development cycle in which we are engaged.
2. Evaluate alternatives, identify and resolve risks: At this point in the development cycle, we evaluate the alternative solutions identified. Any operational or technical issues are identified and addressed here. Risk mitigation is defined and documented during this phase of the spiral.
3. Development: Execution of the objectives for this phase is completed here (e.g., software development, hardware implementation, testing).
4. Plan: This reviews the progress that has been made toward the ultimate project requirements and plans the next development spiral accordingly. Any issues that are identified are addressed before the next development loop begins.

Subsequent development loops will transverse these four stages and focus on the objectives defined for that loop. For example, the first loop through the spiral model will often result in a proof of concept prototype. This initial prototype may be run only in a controlled or laboratory environment with limited features, but key components of the final project can be initially tested. Then, this development loop will expose initial risks and identify possible alternatives going forward. Each subsequent development loop will build upon the initial loop, bringing the project closer to maturity while still providing testable progress along the way.

In the model, radial distance is a measure of effort expended, while the angular distance measures progress. It combines the basic waterfall building block and evolutionary/incremental prototype approaches to software development. The building block activities of design architectural preliminary design review (PDR), detailed design, critical design review (CDR), code, unit test, integration and test, and qualification test are sequentially followed to deliver an initial operational capability (IOC). After IOC, the product is reviewed to determine how its operational capability could be enhanced. Support and maintenance issues are revisited through risk analysis. The product is updated and an operational prototype (s) is demonstrated and validated. The system then goes through an updated waterfall development process with final delivery of a full operational capability (FOC) product. This type of development approach ensures that requirements are defined early and revisited regularly, and risks are identified and managed throughout the development lifecycle, as required (Software Technology Support Center, 2000). Given the complexity of the system proposed in this thesis, a spiral development model will allow for periodic evaluation by all stakeholders. In addition, the model facilitates early identification of risk, which is critically important in a large and complex system.

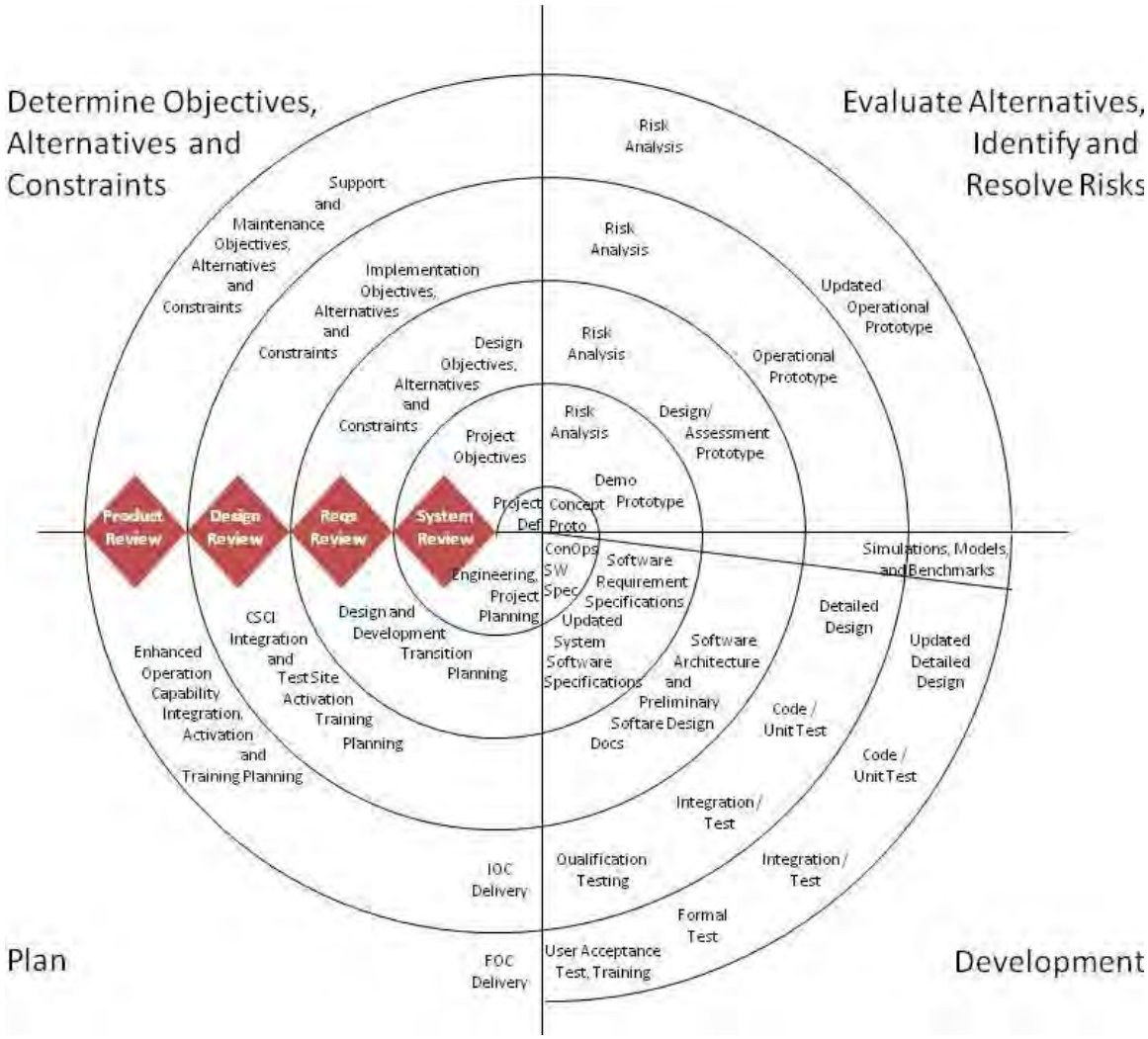

Figure 12. Interoperability Spiral Development Model (from Langford, 2012)

C. SUMMARY

This chapter briefly introduced the system of systems concept along with the models proposed to implement such a program through a development cycle. In addition, it also introduced the spiral development model to specify how the software components of such program would be most efficiently implemented.

IV. NATIONAL SECURITY NETWORK HYPOTHESIS

This chapter will describe in detail the concept of operation proposed in this thesis. It will also identify general requirements by using the engineering spiral approach designed by Barry W. Boehm and introduced in the previous chapter. Finally, this chapter will present a simplified architecture for the proposed CONOPS and discuss information flow (Eisner, 2008).

A. SPIRAL DEVELOPMENT MODEL

The research aim of this thesis is to develop a concept of operations that will detect persons of interest (POI) in real-time as they pass in front of an active monitoring camera such as public cameras on the Internet, DOT traffic cameras, or security cameras near high risk areas (i.e., bridges, tunnels, or major events). The integration of primarily readily available technologies is proposed in the development of this CONOPS. For the purpose of this work, a (POI is a person who poses a threat to national security and who is enrolled by the Terrorist Review and Examination Unit(TREX) into the FBI's consolidated terrorist watch list (as described in Chapter II, **Error! Reference source not found.**).

Integrating the current infrastructure to provide an active ID match of a POI requires a system of systems approach to create a robust operability model. In the following paragraphs, we apply a spiral approach drawn from Langford (2012), which is based on the Boehm model to present the development process from concept to delivery. **Error! Reference source not found.** presents the summary of the spiral approach from a project definition to a robust system of systems. The highlighted portion at the center of the spiral will be addressed in detail below.

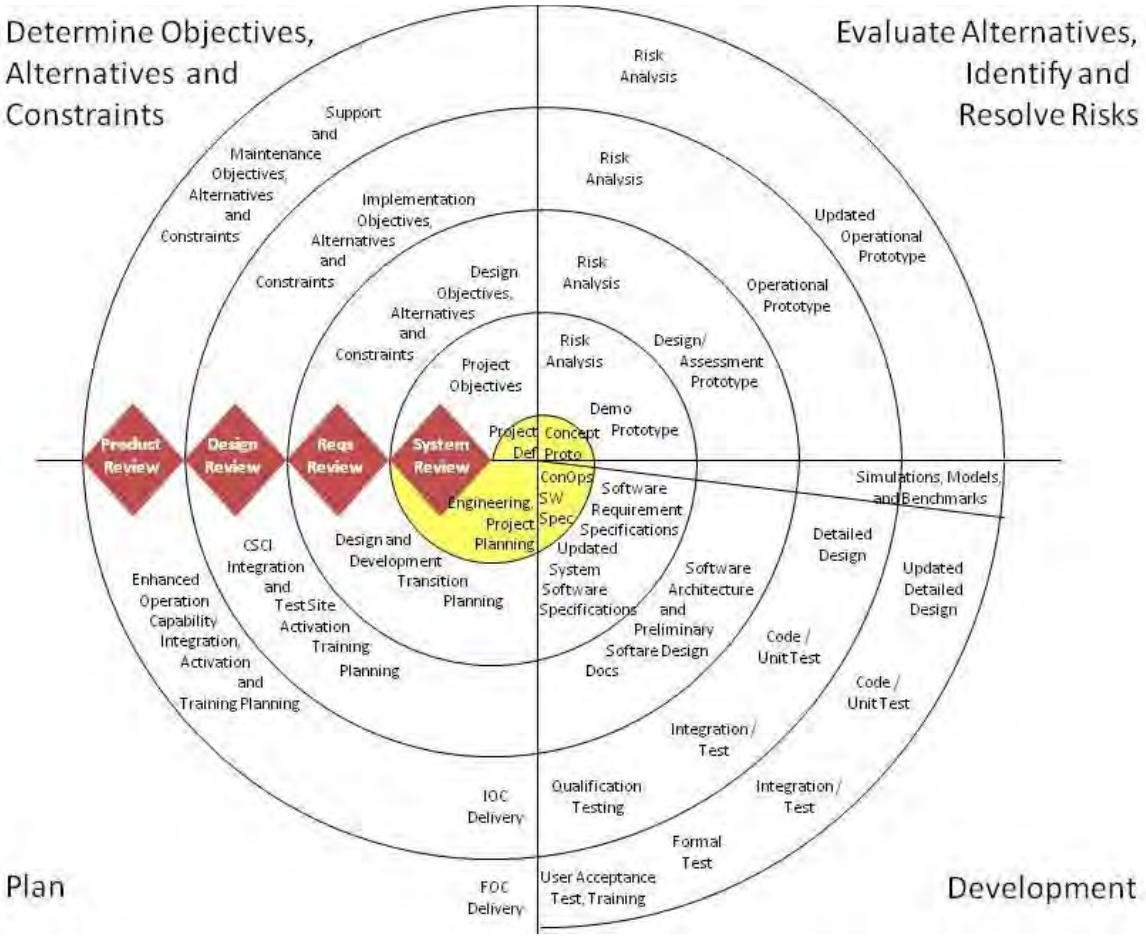

Figure 13. Addressed Portion of Spiral Model (after Langford, 2012)

This thesis will address the first spiral (illustrated in the yellow highlighted portion of **Error! Reference source not found.**) and 1) a project definition, 2) a conceptual prototype, 3) a concept of operations and 4) an engineering and project plan. The thesis will conclude with the system review milestone. Future work would continue the project development around the spiral, with regular risk analysis stages to ensure all stakeholder requirements are met, requirements have not been overlooked, and the project remains on task and on time and budget. The remaining milestones, requirements review, design review, and project review, would be performed at the completion of each spiral (as illustrated in **Error! Reference source not found.**).

1. Project Definition

The project definition stage defines the top-level goals of the project. In this stage, project objectives, alternatives and constraints are defined.

2. Project Objectives

At the highest level, the purpose of the proposed real-time POI identification system is to use biometric facial recognition systems to monitor live video feeds from publicly accessible cameras, such as DOT traffic cameras, social cameras, and security cameras from parking garages, airport terminals, and those set up for major public events, to identify POI present in these feeds and alert the appropriate LE authorities to their presence. To expand further, facial recognition servers will process live cameras and video feeds to determine if a known POI is present. If a POI has been identified by the system, an alert will be generated and sent to the appropriate LE authorities for follow-up. **Error! Reference source not found.** illustrates the components of this high-level project definition.

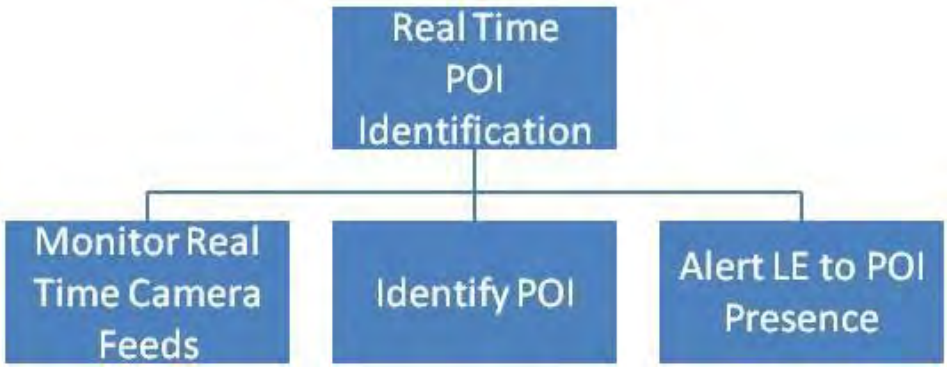

Figure 14. Project Definition

During the project definition phase, we also clearly defined our assumptions to drive the development of the conceptual prototype. The assumptions made here are that the real-time POI identification system can:

- Receive and process streaming live video
- Select from active enrollments in an up-to-date, complete LE database
- Process the image real-time through a facial recognition server
- Send an alert in a universal metadata format that relevant LE/IC agencies can receive

Moreover, the alert will have security protocols in one of three levels:

- Level 3 "GREEN" is dispatched to all authorized users with access to CJIS systems,
- Level 2 "YELLOW" will only distribute a general alert to the responsible LE/IC authority with higher security levels, and
- Level 1 "RED" will only send a general alert with request for information that will be given only to authorized personnel with the appropriate security clearance.

The project definition stage also requires that key project stakeholders be identified. The assumption made for this work is that the FBI is the logical body to govern and manage the networked facial recognition system that will be developed. Currently, CJIS manages the largest biometric repository with its IAFIS system. The proposed facial recognition system can be thought of as a conceptually similar identification system. The experience CJIS has with executing, managing, and maintaining the IAFIS system is applicable to the proposed system. In addition to the FBI, state and local LE officials are also likely stakeholders as they will ultimately be the end users of the system. A working group comprised of members of this community should be created to represent the requirements and interests of these stakeholders to ensure their needs are met.

Funding sources must also be identified in the project definition phase. While funding is a requirement for all acquisitions and the source of money will have to be identified, the selection of an appropriate or available source of funding is out of the scope of this thesis.

- Alternatives: During the project definition phase we also must identify alternatives to the components of the proposed project.
- Constraints: Finally, project constraints must be defined. Project constraints can be defined along with project requirements. Work must be done with project stakeholders to define not only what is included in the project, but what is not included, and how to handle system errors. For example, system constraints would include how to handle network or recognition server outages.

3. Risk Analysis

Risk analysis is completed in each spiral, before the prototypes are developed. For the proposed project, legal, and social analysis must be conducted to ensure privacy rights are protected and to understand the likelihood of public acceptance. Risk of network compromise will be analyzed. Other risks identified in this architecture for consideration are hardware and software compatibility, the speed of throughput, the format of data and images, the latency of delivery, and the rate of technology refresh. Stakeholders may have different requirements, and this difference will pose program risks as well. As with each spiral, risks these will be refined, addressed, and adjudicated.

4. Conceptual Prototyping

The first way to take any idea and make it reality is to illustrate and diagram the approach as well as to review various scenarios. We will prototype our approach by starting with the bare essentials that will be needed to achieve results. Furthermore, we will need a diagram interconnecting a facial recognition database residing behind a secure firewall to live video streaming via the Internet. Then, the information from videos would have to be indexed against information related to a POI. The positive results will be sent via secure metafile to the end user. Illustrating every step of the way will allow the design team to see if the architecture makes sense. Conceptual prototyping allows for the visualization of problems as they arise, which is critical in the design process. **Error! Reference source not found.** incorporates the assumptions outlined in the project definition phase, illustrating the project conceptual prototype.

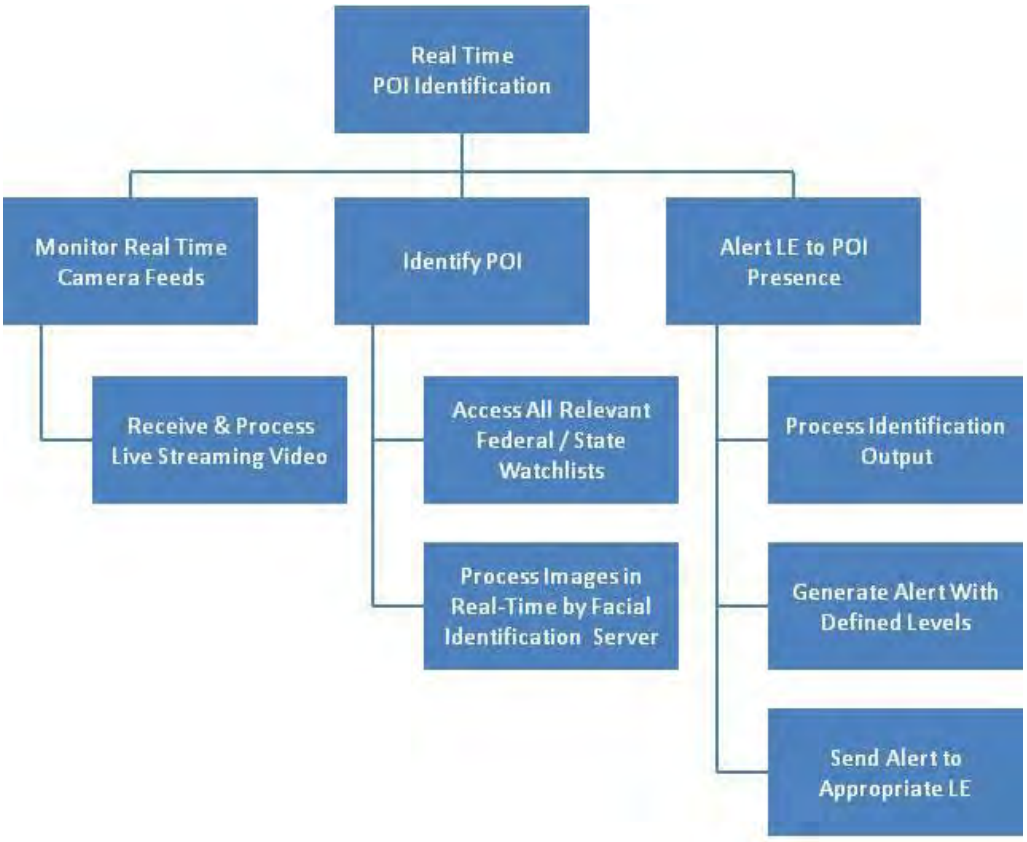

Figure 15. Conceptual Prototype

5. Concept of Operation Development / System Software and Hardware Specification

The fundamental backbone of this concept is a robust, fast, and redundant automated biometrics facial recognition server. Facial Recognition Systems, illustrated at a high level in Figure 15, automatically identifies a person from an image or video frame. This identification is accomplished by comparing features extracted from the image and comparing against those stored in a database. The steps typically involved in the systems are as follows:

- Image capture: Still photographs or frames extracted from live video cameras are used as inputs to the facial recognition system.
- Detection: A face detection system processes the image to determine if a face is present in the captured scene. Those images, or frames for which a face was detected are passed along to the next stage of processing.

- Acceptability testing: Detected faces are further processed to determine if they are acceptable for further processing. For example, most facial recognition systems require a minimum image resolution and minimal angles of alignment with the camera to accurately perform a match.
- Measurement/matching: Measurements of the facial features of the images are computed, and these measurements are statistically compared to those stored in the database index. Matches and their scores are returned.

The algorithms associated with state of the art facial recognition systems continue to evolve, taking into account specific measurements such as skin texture. This evolution continues to improve the accuracy of these systems, which makes them viable for use in CONOPS such as described in this work.

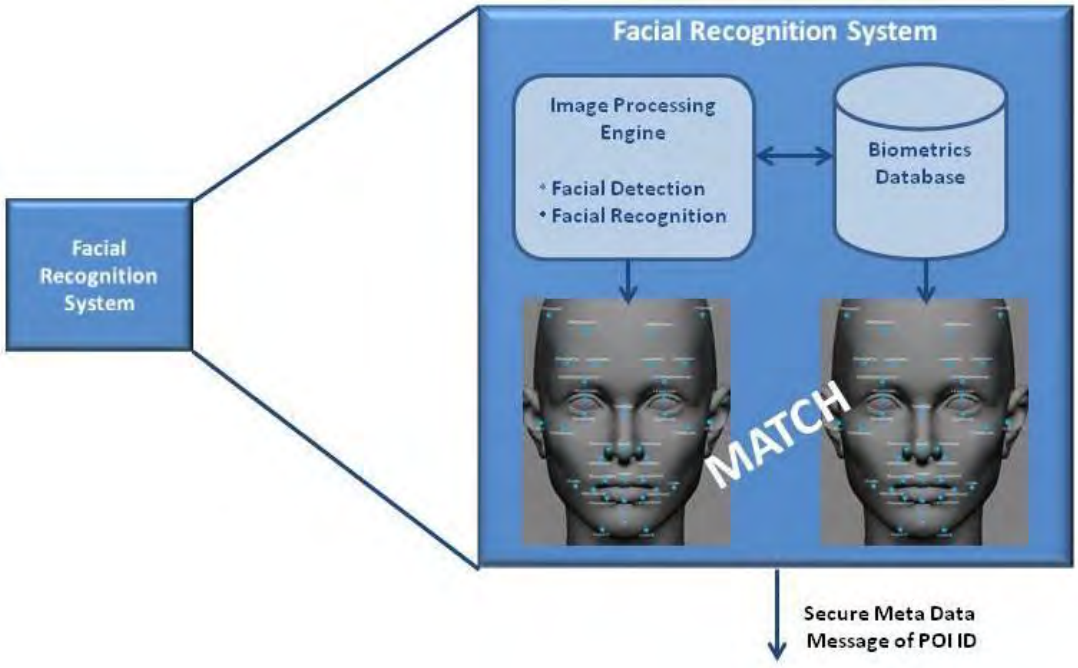

Figure 16. Facial Recognition System (after Anthony, 2014)

The design of the server will go through various developmental spirals, but we will need a software base with an open architecture to work from. Data storage, indexing speeds, and redundant systems will be identified. Biometrics software, operating system software, computer interface, Internet connections, and hardware will be defined.

The facial recognition system can be implemented by integrating two commercially available products: Progeny SPOTR and TAVI. The integration of these two systems will enhance the overall system performance as they utilize different underlying recognition technologies. As of this writing, the author was involved in program managing the Progeny system and TAVI system through Office of Naval Research. During the 20 months of involvement (between 2009 and 2011) with each system, the author had the opportunity to demonstrate and test each concept at TNT Camp Roberts and at Empire Challenge 2010 at Ft. Huachuca military base in Arizona.

The Progeny Surveillance, Persistent Observation and Target Recognition (SPOTR) system utilizes algorithms and techniques that enable object detection and tracking at long range by using standard consumer optics. As compared to traditional methods, the increased range allows improved surveillance of non-cooperative individuals. This range is a key feature as of this proposal is for the use of currently available, low resolution video and camera systems, such as live Internet video feeds at popular locations, general surveillance cameras, and security cameras set up for special events. A successful demonstration of the capability took place at the Empire Challenge in Ft. Huachuca, Arizona.

The Tactical Analysis of Video Imaging (TAVI) system provides automated analysis of surveillance video. System capabilities of interest to this work include face recognition a distances greater than 100m and automatic alerting of security threat events. The system is scalable and adaptable for various mission needs ranging from trailer-based command centers to Android phone-based systems. The integration of the Progeny and TAVI technologies with the proposed network and centralized POI database would provide a robust and adaptable solution to identifying persons of interest in near real-time.

Another requirement is for the CJIS to have the ability to receive streaming live video, process the image real-time through a facial recognition server, and then send an alert in a universal metadata format as required by LE agencies. The alert would have

security protocols in one of three levels, Level 3 "GREEN," Level 2 "YELLOW" and Level 1 "RED" as previously detailed (also see Figure 17).

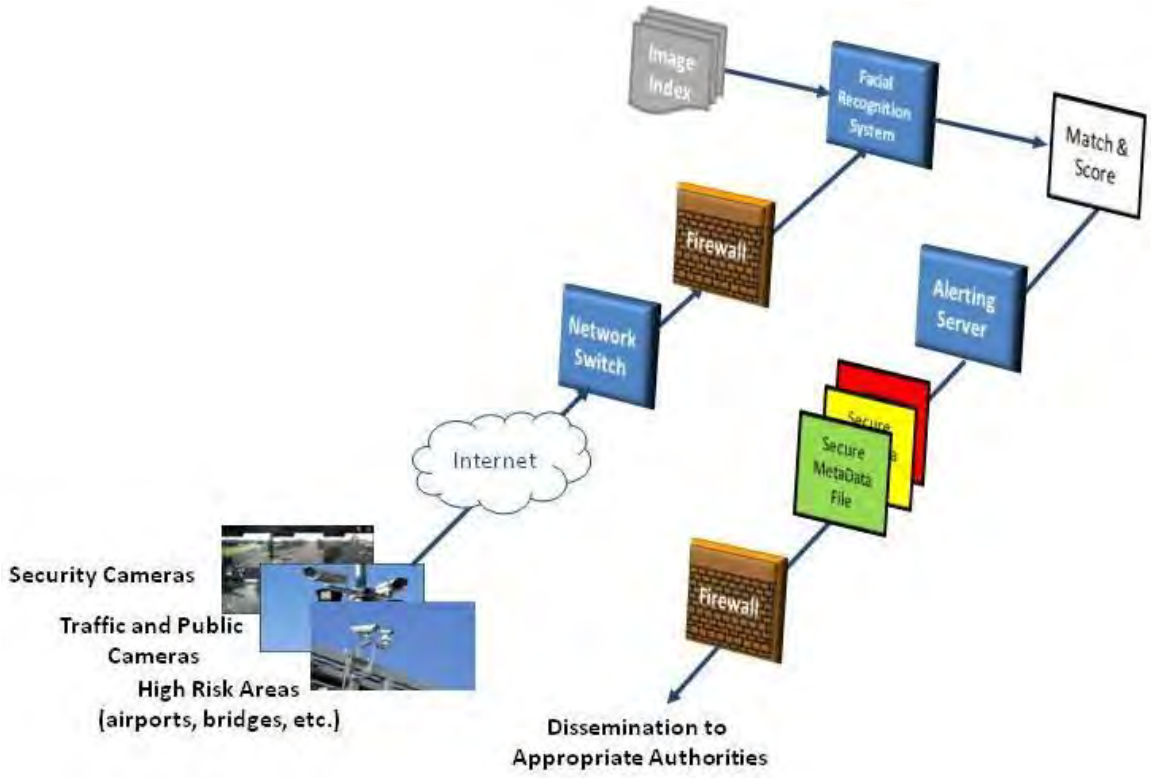

Figure 17. Concept of Operations (after Mayo, 2011)

6. Engineering and Project Planning

Engineering and project planning is essential to ensure all concepts presented are functional and realistic. A project timeline must be thought out and documented. Working groups will be identified for each subsystem. The following project planning questions will be answered.

- How long will this project take from inception to delivery?
- How many prototypes are required before maturity? Where is the funding?
- How much funding is anticipated during each spiral phase through development?

The answers to these questions will identify a preliminary schedule to be used in development.

As mentioned previously, part of the requirements phase will identify the stakeholders, and we have postulated the FBI as the main stakeholder. Having identified a major stakeholder, we can enumerate other steps that would have to take place, such as: developing a pilot program to include testing and acceptance, management, risk management, quality control, and the assembly of working groups. Furthermore, lessons learned would be identified at the conclusion of the pilot phase and based on the outcome. Final preparations would then be made, and cost, technical, and schedule considerations would be formulated.

7. System Review: Milestone

At this stage, the entire spiral development completed to date is reviewed; the outcomes will serve as inputs the next spiral development. All high-risk items are identified and addressed. According to Boehm, the spiral model envisions iterative development as a repeating sequence of steps. Instead of traversing a sequence of analysis, modeling, development, integration, and test just once, software may return over and over to each (Maier, 2009). The system review milestone will pull together the project stakeholders and review the project definition, discuss the risk analysis, review the conceptual prototype, review the concept of operations, and the preliminary engineering and project plan.

B. SUMMARY

A system of systems approach, which features interoperability, is brought forward for consideration in developing this CONOPS based on the identified capability gap. The spiral model, created by Boehm and enhanced by Langford, provides the attention to detail and refinement needed to implement current systems to enhance LE / IC ability to protect national security. The spiral development of this CONOPS will ensure a mature and robust system of systems that can act to identify a POI from live active video streaming from the Internet and match it against active enrollments residing on a secure

LE / IC database. Once a match is found, a secure common metadata file is sent to the appropriate regional LE /IC for further action. Providing real-time monitoring will enhance current LE / IC capabilities in protecting national security.

THIS PAGE LEFT INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

By their nature, passive systems require a significant criminal or terrorist event to occur before they are used to find and identify a POI. Active systems that proactively monitor real-time information feeds could significantly improve security by alerting the LE and IC authorities of the presence of a POI before a crime occurs. While currently both federal and state law enforcement agencies utilize facial recognition technologies to identify a person of interest, these are passive systems that require a request from LE authorities to initiate a search. Additional delays are incurred when multiple requests are needed to search databases that are owned by different government agencies. This increases the time it takes to obtain an actionable match. While there is an ongoing effort to upgrade and consolidate data sharing between federal and state law enforcement agencies, which would address the information flow of data, official requests must still be made to initiate a search.

This word proposes a proactive, real-time augmentation to the current approach; it has the capability of identifying a POI before a threat to national security arises. In addition, by eliminating the formal request process, this proposed capability also significantly reduces the time it takes to identify a POI and enable further investigation. Finally, this type of system can be used to provide additional data, such as patterns of movement of POI to IC investigations. The concept of operations presented in this thesis will significantly enhance current LE / IC capabilities.

B. FUTURE WORK

The concept of operation presented in this thesis can be developed in accordance with the spiral model as presented previously for initial prototyping by utilizing available facial recognition systems to identify a person of interest using low resolution live video streaming from an identified publicly accessible webcam. More research is needed to define resolution requirements to make a positive match to a photograph residing on a

biometric server. Another research opportunity would be to determine if a POI traveling in a vehicle could be identified via installed DOT traffic cameras. It would be necessary to conduct a detailed risk analysis to ensure each development milestone achieves a more refined system. The mitigation of latency issues derived from live video websites is another area for research. A more complete analysis is required to see if a facial recognition server could accurately and effectively scan multiple live video feeds simultaneously and provide accurate results.

APPENDIX DNI COMMUNITY MEMBERS

Appendix A provides a summary description for each of the members of the Intelligence community. These descriptions are provided verbatim from the Office of the Director of National Intelligence (DNI) website (Office of the Directory of National Intelligence, 2012).

A. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INTELLIGENCE & ANALYSIS

The Office of Intelligence and Analysis is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States. DHS Intelligence focuses on five principal areas: improving the quality and quantity of its analysis, integrating the intelligence elements of the department, sharing threat information and assessments with state and local governments and the private sector (Office of Intelligence and Analysis, 2012b).

B. FEDERAL BUREAU OF INVESTIGATION THE NATIONAL SECURITY BRANCH

The National Security Branch (NSB) was established on September 12, 2005 in response to a presidential directive to establish a "National Security Service" that combines the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI under the leadership of a senior FBI official. The NSB strengthens the integration of the FBI's intelligence and investigative missions. Information collected through FBI investigations is analyzed, not just to build a case for prosecution, but for its predictive value. In turn, intelligence drives investigative strategies. In July 2006, the Weapons of Mass Destruction Directorate was created within the NSB to integrate WMD components previously spread throughout the FBI (FBI, 2012d).

C. DEFENSE INTELLIGENCE AGENCY

The Defense Intelligence Agency (DIA) is a Department of Defense combat support agency and an important member of the United States Intelligence community. With over 12,000 military and civilian employees worldwide, DIA is a major producer and manager of foreign military intelligence. It provides military intelligence to warfighters, defense policymakers and force planners in the both Department of Defense and the Intelligence community in support of U.S. military planning and operations and weapon systems acquisition (Defense Intelligence Agency, 2012).

D. CENTRAL INTELLIGENCE AGENCY

The Central Intelligence Agency (CIA) is an independent agency responsible for providing national security intelligence to senior U.S. policymakers (Central Intelligence Agency, 2012).

E. NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

The National Security Agency/Central Security Service (NSA/CSS) is the nation's cryptologic organization that coordinates, directs, and performs highly specialized activities to protect U.S. information systems and to produce foreign signals intelligence information. A high-technology organization, NSA is at the forefront of communications and information technology (National Security Agency, 2012).

F. DRUG ENFORCEMENT ADMINISTRATION OFFICE OF NATIONAL SECURITY INTELLIGENCE

The Office of National Security Intelligence (ONSI) is responsible for providing drug-related information responsive to IC requirements. DEA/ONSI establishes and manages centralized tasking of requests for and analysis of national security information obtained during the course of DEA's drug enforcement (Drug Enforcement Administration, 2012).

G. DEPARTMENT OF TREASURY, OFFICE OF INTELLIGENCE & ANALYSIS

The Office of Intelligence and Analysis (OIA) was established by the Intelligence Authorization Act for FY2004. The act specifies that OIA shall be responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of the Department of the Treasury (Office of Intelligence & Analysis, 2012a).

H. DEPARTMENT OF STATE, BUREAU OF INTELLIGENCE & RESEARCH

The Bureau of Intelligence and Research (INR) provides the Secretary of State with timely, objective analysis of global developments as well as real-time insights from all-source intelligence. It serves as the focal point within the Department of State for all policy issues and activities involving the intelligence community (U.S. Department of State, 2012).

I. NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

The National Geospatial-Intelligence Agency (NGA) provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. Information collected and processed by NGA is tailored for customer-specific solutions (National Geospatial-Intelligence Agency, 2012).

J. NATIONAL RECONNAISSANCE OFFICE

The National Reconnaissance Office (NRO) designs, builds and operates the nation's reconnaissance satellites. NRO products, which are provided to an expanding list of customers like the Central Intelligence Agency (CIA) and the Department of Defense (DOD), can warn of potential trouble spots around the world, help plan military operations, and monitor the environment (National Reconnaissance Office, 2012).

K. DEPARTMENT OF ENERGY, OFFICE OF INTELLIGENCE & COUNTERINTELLIGENCE

The Office of Intelligence and Counterintelligence provides the secretary, staff, and other policymakers within the department timely, technical intelligence analyses on all aspects of foreign nuclear weapons, nuclear materials, and energy issues worldwide (Department of Energy, 2012).

L. UNITED STATES AIR FORCE

Air Force Intelligence plays a critical role in the defense of our nation, providing aerial reconnaissance and surveillance in every conflict and contingency operation since its establishment as a separate service in 1947. Air Force aerial reconnaissance and surveillance began with open cockpits and observers drawing crude maps as they flew and rapidly advanced to photographic reconnaissance being taken from converted fighter and bomber aircraft (United States Air Force, 2012).

M. UNITED STATES ARMY

The U.S. Army Intelligence department (G2) is responsible for policy formulation, planning, programming, budgeting, management, staff supervision, evaluation, and oversight for intelligence activities for the Department of the Army. The G2 is responsible for the overall coordination of the five major military intelligence (MI) disciplines within the Army: imagery intelligence, signals intelligence, human intelligence, measurement and signature intelligence, and counterintelligence and security countermeasures (United States Army, 2012).

N. UNITED STATES MARINE CORPS

Within the Marine Corps, intelligence is an inherent component of the command decision-making process. Under Marine Corps doctrine, intelligence is considered the foundation on which the operational effort is built and the premise on which all training, doctrine, and equipment are developed. The Marine Corps Intelligence mission is to

provide commanders at every level with seamless, tailored, timely, and mission-essential intelligence and to ensure this intelligence is integrated into the operational planning process (United States Marine Corps, 2012).

O. UNITED STATES NAVY

Established on March 23, 1882, Naval Intelligence is the oldest continuous serving U.S. intelligence service. It is a global intelligence enterprise of over 20,000 uniformed and civilian personnel. The Naval Intelligence primary production organization, the Office of Naval Intelligence (ONI), located at the National Maritime Intelligence-Integration Office (NMIO) in Suitland, Maryland, is the lead Department of Defense production center for maritime intelligence. ONI supports a variety of missions including U.S. military acquisition and development, counter-terrorism, counter-proliferation, counter-narcotics, customs enforcement and, through partnerships and information sharing agreements with the U.S. Coast Guard and U.S. Northern Command, Homeland Security and Homeland Defense. While ONI is the largest Naval Intelligence organization with the largest concentration of Naval Intelligence civilians, most of Naval Intelligence is comprises active duty military personnel, who are serving throughout the world (United States Navy, 2012).

P. UNITED STATES COAST GUARD

The Coast Guard's broad responsibilities include protecting citizens from the sea (maritime safety), protecting America from threats delivered by the sea (maritime security), and protecting the sea itself (maritime stewardship). The Coast Guard's persistent presence in the maritime domain, due to its diverse mission sets and broad legal authorities, allows it to fill a unique niche within the Intelligence community. Because of its unique access, emphasis, and expertise in the maritime domain Coast Guard Intelligence can collect and report intelligence that not only supports Coast Guard missions, but also supports national objectives. Coast Guard Intelligence strives to create decision advantage to advance U.S. interests by providing timely, actionable, and

relevant intelligence to shape Coast Guard operations, planning, and decision-making, and to support national and homeland security intelligence requirements (United States Coast Guard, 2012).

LIST OF REFERENCES

Anthony, S. (2014, March 19). Facebook's facial recognition software is now as accurate as the human brain, but what now? *Extreme Tech*. Retrieved from http://www.extremetech.com/extreme/178777-facebooks-facial-recognition-software-is-now-as-accurate-as-the-human-brain-but-what-now

Baker, T. J. (2012, May). Biometrics for intelligence-led policing: The coming trends. *The Police Chief Magazine*. Retrieved from http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2358&issue_id=42011

Bertolini, P. (2012). *CLEMIS law enforcement applications and systems*. Oakland County, MI: Chief Information Officers of the States.

Boehm, B. (1986, August). A spiral model of software development and enhancement. *ACM SIGSOFT Software Engineering Notes*, *11*(4), pp. 14–24. Retrieved from http://dl.acm.org/citation.cfm?id=12948

Bruegge, R. W. (2010). Facial recognition and identification initiatives. Presented at 2010 Biometrics Conference, Tampa, FL. Retrieved from http://biometrics.org/bc2010/

Central Intelligence Agency. (2012). About CIA. Retrieved from http://www.cia.gov/about

Chachere, V. (2001, February 13). Biometrics used to detect criminals at Super Bowl. *ABC News*. Retrieved from http://abcnews.go.com/Technology/story?id=98871&page=1

COPSync. (2012). COPSync. Retrieved from http://www.copsync.com

Criminal Justice Information services Division. (2010, August 25). Law Enforcement National Data Exchange (N-DEx). Retrieved from http://www.ijis.org/docs/N-DEX%20information-slides_v08252010.pdf

Department of Energy. (2012). Office of Intelligence and Counterintelligence. Retrieved from http://www.ch.doe.gov/offices/OCI/

Defense Intelligence Agency. (2012). About DIA. Retrieved from http://www.dia.mil/about

Department of the Air Force. (2000). System life cycle and methodologies. In *Guidelines for Successful Acquisition and Management of Software-Intensive Systems*. Version 3.0. Washington, DC: Defense Acquisition University.

Drug Enforcement Administration. (2012). Intelligence. Retrieved from http://www.justice.gov/dea/programs/intelligence.htm

eAGENT Client Mobile. (2012). Client mobile. Retrieved from http://www.diversecomputing.com/products/eagent/eAgent-client-mobile-ncic-access

EGGMAN Technologies. (2012). Mobile surveillance with PTZ and audio. Retrieved from http://www.eggmantechnologies.com/

Eisner, H. (2008). *Essentials of project and systems engineering management.* Hoboken, NJ: John Wiley & Sons.

Endler, M. (2012, September 11). FBI's Facial Recognition Program: Better security through biometrics. *InformationWeek Government*. http://www.darkreading.com/risk-management/fbis-facial-recognition-program-better-security-through-biometrics/d/d-id/1106236?

Federal Bureau of Investigation Criminal Justice Information Services Division. (2009). Criminal Justice Information Network. Retrieved from http://www.cjin.nc.gov/library/pdf/NDExPresentationRaleigh102909.pdf

Federal Bureau of Investigation. (2009). *The Federal Bureau of Investigation's Terrorist Watchlist nomination practices*. Washington, DC: Author.

Federal Bureau of Investigation. (2012a). Fingerprints & other biometrics: Next generation identification. Retrieved from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2

Federal Bureau of Investigation. (2012b). Integrated automated fingerprint identification system. Retrieved November 04, 2012, from http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis

Federal Bureau of Investigation. (2012c). National Crime Information Center. Retrieved from http://www.fbi.gov/about-us/cjis/ncic

Federal Bureau of Investigation. (2012d). National Security Branch. Retrieved from http://www.fbi.gov/about-us/nsb

Free live webcams. (2012). Opentopia. Retrieved from http://www.opentopia.com

Identifier interoperability: A report on two recent ISO activities. (2012, May). http://www.dlib.org/dlib/april06/paskin/04paskin.html

Jones, G. (2010, June 03). NSW government recording features for facial recognition. *The Daily Telegraph*. Retrieved from http://www.dailytelegraph.com.au/news/national/nsw-government-recording-features-for-facial-recognition/story-e6freuzr-1225874819392

Kaplan, J. M. (2006). A new conceptual framework for net-centric, enterprise-wide, system-of-systems engineering. Washington DC: National Defense University Center for Technology and National Security Policy.

Kenyon, H. (2010, August 24). Gates orders increased data sharing to protect military families. *Government Computer News*. Retrieved from http://s.tt/1bcHD http://gcn.com/articles/2010/08/24/dod-to-increase-data-sharing-to-protect-personnel-and-facilities.aspx

L-1 Identity Solutions. (2012). Biometrics: Capturing, managing and moving biometric data for positive, rapid ID and tracking of persons of interest. Retrieved from http://wwwl1id.com/pages/17-biometrics

Langford, G. O. (2012). *Engineering systems integration: Theory, metrics and methods*. Baca Raton, FL: CRC Press.

Maier, M. W. (2009). *The art of systems architecting*. 3rd ed. Washington, DC: CRC Press.

Mayo, K. (2011, November). RISC: Mobile fingerprint ID goes national. *Evidence Technology Magazine*. Retrieved from http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=655

National Criminal Intelligence Resource Center. (2011, October). Fusion process catalog of services. (2011, October). Retrieved from http://www.ncirc.gov/documents/Fusion_Process_Catalog_of_Services.pdf

National Geospatial-Intelligence Agency. (2012). National Geospatial-Intelligence Agency. Retrieved from https://www.nga.mil/Pages/default.aspx

National Reconnaissance Office. (2012). National Reconnaissance Office. Retrieved from http://www.nro.gov

National Security Agency. (2012). National Security Agency. Retrieved from http://www.nsa.gov

Office of Intelligence & Analysis. (2012a). About. Retrieved from http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Intelligence-Analysis.aspx

Office of Intelligence and Analysis. (2012b). About Office of Intelligence and Analysis. Retrieved from http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm

Office of the Directory of National Intelligence. (2012). Members of the IC. Retrieved from http://www.dni.gov/index.php/intelligence-community/members-of-the-ic

Paskin, N. (2006, April). Identifier interoperability: A report on two recent ISO activities. *D-Lib Magazine*, *12* no. 4. Retrieved from http://www.dlib.org/dlib/april06/paskin/04paskin.html

Public Dropcams. (2012). See what's live on Dropcam. Retrieved from https://www.dropcam.com/cameras/public

Protect America Act. Public Law 110-55 (2007).

Reardon, S. (2012, September 07). FBI launches $1 billion face recognition project. *New Scientist* (2880). http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html#.U1h3WhCa9Oo

Schultz, G. (2012, February 06). Increasing use of facial recognition software spurs privacy concerns. *California Watch*. Retrieved from http://californiawatch.org/dailyreport/increasing-use-facial-recognition-software-spurs-privacy-concerns-14763

Steele, E., & Angwin, J. (2011, August 16). Device raises fear of facial profiling. *Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html

Surveillance, Persistent Observation, and Target Recognition. (2012). Surveillance, Persistent Observation, and Target Recognition (SPOTR™). Retrieved from http://www.spotrtech.com

United States Air Force. (2012). United States Air Force. Retrieved from http://www.af.mil

United States Army. (2012). United States Army. Retrieved from http://www.army.mil

United States Coast Guard. (2012). United States Coast Guard. Retrieved from United States Coast Guard: http://www.uscg.mil/

United States Department of Homeland Security. (2011). *2011 National network of fusion centers final report*. Washington, DC: Author.

United States Department of Homeland Security. (2012). National network of fusion centers fact sheet. Retrieved from http://www.dhs.gov/national-network-fusion-centers-fact-sheet

United States Department of State. (2012). Bureau of Intelligence & Research. Retrieved from http://www.state.gov/s/inr/

United States Marine Corps. (2012). United States Marine Corps. Retrieved from http://www.marines.mil

United States Navy. (2012). United States Navy. Retrieved from http://www.navy.mil

Wikipedia. (2012). United States Intelligence community. Retrieved from http://en.wikipedia.org/wiki/United_States_Intelligence_Community

What facial recognition technology means for privacy and civil liberties. Statement before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law, 112th Cong., (2012) (testimony of Jerome M. Pender). Retrieved from http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties

WVHTC Foundation. (2013). Advanced Technology Group: Tactical Analysis of Video Imagery (TAVI). Retrieved from WVHTC Foundation: http://www.wvhtf.org/departments/advanced_tech/projects/tavi.asp

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California